CONDUCTING A PRIVACY IMPACT ASSESSMENT ON SURVEILLANCE CAMERA SYSTEMS (CCTV)
Principle 2 of the surveillance camera code of practice states that the use of a surveillance camera system must take into account the effect on individuals and their privacy, with regular reviews to ensure its use remains justified. The best way to ensure this is by conducting a privacy impact assessment before the system is installed and when a new camera is being added on to an existing system. This will assist in managing any privacy issues the use of the surveillance system might have.

A privacy impact assessment (PIA) enables operators to unpick risks to compliance with the Data Protection Act 1988 and the Human Rights Act 1998. The PIA should initially consider the pressing need that the system seeks to address and the impact that recording may have on individual's privacy. It is important to decide whether the proposed system can be justified as proportionate to the reason it is needed.

In undertaking a privacy impact assessment you must take into consideration your obligations under the Data Protection Act 1998 and follow the guidance provided in the Information Commissioner’s Office’s (ICO) CCTV code of practice.

This privacy impact assessment template is specifically for those organisations that must have regard to the surveillance camera code of practice under the Protection of Freedoms Act 2012. It also helps organisations to address their data protection and human rights obligations.

A PIA does not always have to be conducted as a completely separate exercise and it can be incorporated into project planning or other management and review activities.

In deciding whether to conduct a PIA and its scope, consideration must be given to the nature and scope of the surveillance camera activities and their potential to impact on the privacy rights of individuals.

A PIA should be considered when you are reviewing your surveillance camera systems and when you are considering introducing new technology connected to them.

A privacy impact assessment should be considered when any of the following apply:

- When you are introducing a new surveillance camera system.
- If you are considering introducing new or additional technology that may affect privacy (e.g. automatic number plate recognition (ANPR), body worn cameras, unmanned aerial vehicles (drones), megapixel or multi sensor very high resolution cameras).
- When you are changing the location or field of view of a camera or other such change that may raise privacy concerns.
- When you are reviewing your system to ensure that it is still justified. It is recommended that you review your system annually (see ICO CCTV Code of Practice and Surveillance Camera Code of Practice Principle 10).
- If you are considering the capture of an additional identifier such as vehicle registration mark to enable ANPR.
- The activity or change will engage heightened privacy concerns such as voice recording and biometric recognition such as facial and gait recognition.
- If your system involves any form of cross referencing to other collections of personal information.
- If your system involves more than one company or agency undertaking activities either on your behalf or in their own right.
- When you change the way in which the recorded images and information is handled, used or disclosed.
- When you increase the area captured by your surveillance camera system.
- When you change or add an end user or recipient for the recorded information or information derived from it.
Description of proposed surveillance camera system

Provide an overview of the proposed surveillance camera system

This should include the following information:

- An outline of the problem the surveillance camera system is trying to resolve.
- Why a surveillance camera system is considered to be the most effective way to solve the issues.
- How the surveillance camera system will be used to address the problem (identified above).
- How success will be measured (i.e. evaluation: reduction in crime, reduction of fear, increased detection etc).

In addition, consideration must be given to proportionality, legality, accountability and necessity. Any interference by a public authority of an individual’s rights must be justified.

Therefore the following questions must be considered as part of a PIA:

- Is the surveillance activity established on a proper legal basis and is it undertaken in accordance with the law?
- Is the surveillance activity necessary to address a pressing need, such as public safety, crime prevention or national security?
- Is it justified in the circumstances?
- Is it proportionate to the problem that it is designed to deal with?

If the answer to any of these questions is no, then the use of surveillance cameras is not appropriate.

Otherwise please proceed to complete the template below.
PRIVACY IMPACT ASSESSMENT TEMPLATE

The privacy impact assessment template comprises two parts.

Level one considers the general details of the surveillance camera system and supporting business processes, level two considers the specific implications for the installation and use of cameras.

Template – Level One

Location of surveillance camera system being assessed:

A CCTV system is installed inside the following 7 designated Kent Police custody suites: Medway, North Kent, Maidstone, Tonbridge, Canterbury, Folkestone, Margate.

Date of assessment: 31.03.2019
Review date: 31.03.2020
Name of person responsible: Inspector 9219 Colin Piddock

Data Protection Act 1998 and Surveillance Camera Code of Practice 2013

1. What is the organisation’s purpose for using the surveillance camera system and what are the issues that the system aims to address? Evidence should be provided which should include relevant available information, such as crime statistics for the previous 12 months, the type, location, times and numbers of crime offences, housing issues relevant at the time, community issues relevant at the time and any environment issues relevant at the time.

CCTV is operated by Kent Police inside its 7 designated custody suites and is used as a proportionate response to provide a safe working environment for detainees, staff and visitors. The use of custody CCTV aims to reduce the incidents of self-harm or criminal damage committed by detainees as well as act as a deterrent against spontaneous outbreaks of violence and disorder. Within each of the 7 custody suites there are a number of fixed position cameras that have the ability to capture both sound and visual recordings in high definition. The CCTV cameras can be used to capture identifiable images of an individual and will only be used by staff trained in its use. The custody CCTV can also be used to support a complaint made against the police or a post incident investigation undertaken by the Independent Office for Police Conduct (IPOC) or our own internal Professional Standards Department. CCTV footage that is downloaded will be kept in accordance with Kent Police Policy Q01e and the NPCC retention schedule.

2. Can a surveillance camera technology realistically deliver these benefits? State why the use of surveillance cameras will deliver these benefits in practice including evidence to justify why that would be likely to be the case.

Yes the custody CCTV consistently delivers the benefits described above.
3. What are the views of those who will be under surveillance? Please outline the main comments from the public resulting from your consultation – some consultation should be undertaken in the area being considered for a surveillance camera scheme. This can often be achieved by existing local consultation mechanisms such as local area committees, police beat meetings; but, if necessary depending on the privacy intrusion of the surveillance in question, other mechanisms could be considered such as face to face interviews, questionnaires being sent to residents/businesses and addressing focus groups, crime & disorder partnerships and community forums.

Intrusion of the custody CCTV cameras is limited to the enclosed police premises to which access is restricted to detained persons, custody staff, legal representatives and authorised visitors only. Therefore no public engagement was undertaken prior to the installation of the system. In addition CCTV warning signs are present in each custody suite and any representations about the use of CCTV within a custody suite will be addressed by the custody sergeant.

4. Have other less privacy-intrusive solutions such as improved lighting been considered? There is a need to consider other options prior to the use of cameras. For example, could improved lighting deliver the same benefit? Does the camera operation need to be 24/7? Where these types of restrictions have been considered, provide reasons for not adopting them and opting to use surveillance cameras as specified.

Other approaches such as improved lighting would not achieve the same safety benefits as the custody CCTV.

5. What are the benefits to be gained from using surveillance cameras? Give specific reasons why this is necessary compared to other alternatives. Consider if there is a specific need to prevent/detect crime in the area. Consider if there would be a need to reduce the fear of crime in the area, and be prepared to evaluate.

The use of custody CCTV is proven to be an effective tool in improving the safety of the custody environment and its installation and use is supported by the College of Policing Authorised Professional Practice. Custody CCTV is also effective in investigating complaints or civil claims made against the police involving incidents that have taken place in custody.

6. What are the privacy issues arising from this surveillance camera system? State the main privacy issues relating to this particular system. For example, the extent of information recorded, whether it will be only on those who are suspects or include those who are not, concerns arising from its use, retention and disclosure, likely expectations of those under surveillance and impact on their behaviour, level of intrusion into their lives, effects on privacy if safeguards are not effective.

The custody CCTV system operates through a series of fixed cameras installed throughout each custody suite. The CCTV is recorded onto a hard disc drive and the images remain on the hard disc drive for a period of 31 days after which they are automatically recorded over unless requested as part of an incident or investigation. Then the relevant images will be identified, retrieved and archived in accordance with Kent Police Policy Q01e and the NPCC retention schedule.

7. Have any privacy by design features been adopted to reduce privacy intrusion? Could any features be introduced as enhancements? State the privacy enhancing technical and other features that have been identified, considered and accepted or rejected. For example, has consideration been given to the use of technical measures to limit the acquisition of images, such as privacy zones installed on cameras that overlook residential properties, etc? If these have not been adopted, provide a reason.

During the installation of the custody CCTV safeguards were put into place to reduce privacy intrusion. The first of these involve the images obtained from cameras operating inside of the custody cells which are viewed via television monitors located within the custody offices. No persons other than police personnel have access to the custody offices and when the image is viewed on the television monitor the area of the cell covering the toilet is pixelated in order to maintain the dignity of the detainee using...
Conducting a Privacy Impact Assessment on surveillance camera systems (CCTV) (07.17)
12. What future demands may arise for wider use of images and how will these be addressed? Consider whether it is possible that the images from the surveillance camera scheme will be used for any other purpose (e.g. traffic monitoring, enforcement, ANPR) in future and how such possibilities will be addressed. Will the cameras have a future dual function?

As part of the development of future digital media technology it is likely the demand for custody images will increase with the potential for custody images to be used to investigate and detect crimes or incidents that occur outside of the custody environment for example facial recognition technology to identify potential suspects. Kent Police will comply with any new legislation that increases the use and scope of custody CCTV images to ensure minimum intrusion into people's private lives is maintained.

Human Rights Act 1998

Section 6(1) of the Human Rights Act 1998 (HRA) provides that it is unlawful for a public authority to act in a way which is contrary to the rights guaranteed by the European Convention on Human Rights. Therefore in addition to the above, if you are a public authority, you must make sure that your system complies with the requirements under the HRA.

1. Is the system established on a proper legal basis and is it operated in accordance with the law? State the statutory or other powers which provides the basis for the activity.


2. Is the system necessary to address a pressing need, such as public safety, crime prevention or national security? Articulate the problem and why this is a pressing concern.

The custody CCTV system is an essential tool used by police to maintain the safety and security of people who are detained, work or visit a Kent Police custody suite. The use of custody CCTV is supported by the Independent Office for Police Conduct (IOPC) report which examined deaths in police custody and made a series of recommendations in order to reduce deaths or serious incidents which is referenced in recommendation 7:

'Police forces should ensure that CCTV is available in at least one cell in the custody suite, to be used when a detainee is identified as being at risk, and, where available, that it is fully operational. Independent custody visitors should check that CCTV is operational when carrying out their custody visits.'

3. Is it justified in the circumstances? Provide the justification.

The use of CCTV in Kent custody suites is justified as one of the aims of Kent Police is to safeguard the welfare of people who have been arrested and detained in one of Kent's 7 custody suites.

4. Is it proportionate to the problem that it is designed to deal with? Explain why the level of privacy interference is proportionate to the overall privacy impact.

The use of CCTV in Kent custody suites is proportionate as it will be used to keep people safe who are detained, work or visit one of Kent's 7 custody suites and its installation and use complies with current legislation.
5. **Do any of these measures discriminate against any particular sections of the community?**

Detail whether the proposed surveillance will have a potential discriminatory or disproportionate impact on a section of the community. For example, establishing a surveillance camera system in an area with a high density of one particular religious or ethnic group.

The use of CCTV in Kent custody suites is carried out in accordance with current legislation and complies with Home Office guidance around Article 8 of the European Convention of Human Rights to ensure the gathering of data is proportionate, legal, accountable, necessary and likely to cause minimum invasion to privacy and does not discriminate any particular group or individual and retention of custody CCTV footage is in carried out in accordance with Kent Police Policy Q01e and the NPCC retention schedule.
PRIVACY IMPACT ASSESSMENT LEVEL TWO

The Level 2 privacy impact assessment template is designed to give organisations a simple and easy to use document to record various placements and devices on their surveillance camera system and to demonstrate the recognition and reduction of ‘risk’ to privacy impact across their network or system.

This document seeks to satisfy the privacy impact assessment in principle two of the Surveillance Camera Code of Practice.

Principle 2 - The use of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

When looking at the obligation under the code a risk assessment methodology has been developed to help organisations identify any privacy risks to individual or specific group of individuals (e.g. children, vulnerable people), compliance risks, reputational risks to the organisation and non-compliance with the Protection of Freedoms Act and/or the Data Protection Act.

A system that consists of static cameras in a residential housing block will generally present a lower risk than a system that has multiple High Definition Pan Tilt and Zoom (PTZ) cameras. However, the privacy impact assessment should help identify those cameras (irrespective of the type) that may be directed at a more vulnerable area (e.g. a children’s play area) and therefore presenting a higher privacy risk. This approach allows the organisation to document a generic approach to the intrusion into privacy, catalogue your cameras by type and location, and finally identify any cameras that present specific privacy risks and document the mitigation you have taken.

An example of a risk assessment guide is shown in Appendix One

When undertaking a privacy impact assessment, it is important to be able to confirm where the organisation’s cameras are sited. The system asset it is considered to be good practice for all organisations to maintain an asset register for all of their devices. This allows the system owner to record each site and equipment installed therein categorised in a manner to lead into the level two process.

If any new site or installation sits outside of the pre-defined fields, then new categories can be added as required

Overall step one and step two will cover the uses of devices of the system. However, it may not be practicable to publically list or categorise each individual asset.

A register can be developed to capture the information required.
### Template – Level Two

#### Step 1 (definition of camera types utilised)

**Cameras Specification:** System operator owner should include below all camera types and system capabilities (e.g. static, PTZ, panoramic, ANPR) and their likely application and expected use. This will differ by organisation, but should be able to reflect a change in the cameras ability due to upgrade.

Please see example below:

<table>
<thead>
<tr>
<th>ID</th>
<th>Camera types</th>
<th>Makes and models used</th>
<th>Amount</th>
<th>Description</th>
<th>Justification and expected use</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>High Definition Static.</td>
<td>Mixture of Axis P3364 V6 cameras and Axis P3364 V12.</td>
<td>309</td>
<td>Static images, no movement or zoom function. High Definition.</td>
<td>The 309 fixed CCTV cameras are installed within the following 5 custody suites: Tonbridge, Maidstone, Canterbury, Folkestone and Margate. The custody cameras are regularly monitored by staff working in custody to ensure the safety of detainees, staff and visitors.</td>
</tr>
<tr>
<td>2.</td>
<td>Standard.</td>
<td>Vicon, model no V661D-312N-1-P.</td>
<td>134</td>
<td>Static images, no movement or zoom function.</td>
<td>The 134 fixed CCTV cameras are installed within Medway custody suite. The custody cameras are regularly monitored by staff working in custody to ensure the safety of detainees, staff and visitors.</td>
</tr>
</tbody>
</table>
**Step 2 (location assessment)**

**Location:** Each system operator/owner should list and categorise the different areas covered by surveillance on their system. This list should use the specifications above which ID (types) are used at each specific location.

<table>
<thead>
<tr>
<th>CAT</th>
<th>Location type</th>
<th>Camera types used</th>
<th>Amount</th>
<th>Recording</th>
<th>Monitoring</th>
<th>Assessment of use of equipment (mitigations or justifications)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.</td>
<td>CCTV is used extensively throughout all 7 custody suites.</td>
<td>Static HD and Standard.</td>
<td>24hrs</td>
<td>24hrs by trained custody staff.</td>
<td>The use and monitoring of custody CCTV cameras is to ensure the safety of detainees, staff and visitors who attend on of Kent's 7 custody suites. Each suite has CCTV warning signs to notify people CCTV is in operation.</td>
<td></td>
</tr>
<tr>
<td>B.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>F.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>G.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>J.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>K.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 3 (Cameras where additional mitigation required)**

**Asset register:** It is considered to be good practice for all organisations to maintain an asset register for all of their devices. This allows the system owner to record each site and equipment installed therein categorised in a manner to lead into the level two process.

If any new site or installation sits outside of the pre-defined fields, then new categories can be added as required.

Overall step one and step two will cover the uses of devices of the system. However, it may not be practicable to publically list or categorise each individual asset.

Please document here any additional mitigation taken on a camera or system to ensure that privacy is in line with the ECHR requirements.

<table>
<thead>
<tr>
<th>Camera number</th>
<th>Reviewed</th>
<th>Camera type</th>
<th>Location category</th>
<th>Further mitigation/ comments (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Conducting a Privacy Impact Assessment on surveillance camera systems (CCTV) (07.17)**

<table>
<thead>
<tr>
<th>Camera number</th>
<th>Reviewed Camera type</th>
<th>Location category</th>
<th>Further mitigation/ comments (optional)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Step 4 (Mitigation for specific cameras that have high privacy risks)**

For the occasion where there is a very high impact an Authority may wish to conduct an extensive PIA of specific installations and the site and have it fully documented.

**PIA for specific installations**

Camera number

Camera location

<table>
<thead>
<tr>
<th>Privacy risk(s)</th>
<th>Solution</th>
<th>Outcome (Is the risk removed, reduced or accepted)</th>
<th>Justification (Is the impact after implementing each solution justified, compliant and proportionate to the aim of the camera?)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Agreed with: Adrian Futers, Head of Information Security & Governance

Signature 46060164

Date 17/05/19

Review date 17/05/20
**APPENDIX ONE: PRIVACY RISK ASSESSMENT MATRIX**

Scoring could be used to highlight the risk factor associated with each site if done utilising the risk matrix example shown below.

**Matrix Example:**

<table>
<thead>
<tr>
<th>Location Types</th>
<th>Camera Types (low number low impact – High number, High Impact)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A (low impact)</td>
<td><img src="image" alt="Matrix Example" /></td>
</tr>
<tr>
<td>Z (high impact)</td>
<td></td>
</tr>
</tbody>
</table>
## APPENDIX TWO: STEPS INVOLVED IN CONDUCTING A PRIVACY IMPACT ASSESSMENT

1. Understand and establish the pressing need through problem analysis. Consider all possible solutions e.g. lighting, target environmental, hardening etc. If a surveillance camera system identified as most appropriate, then conduct a privacy impact assessment.

2. Identify the legal basis for the surveillance camera system.

3. Identify the personal information the system will gather and consider how it will be used.

4. Identify the level of privacy intrusion and privacy risks through consultation with stakeholders and the public.

5. Weigh up the necessity and proportionality of your system against any privacy intrusion.

6. Find ways to reduce the privacy intrusion to proportionate levels or decide not to proceed.

7. Review your system regularly (at least annually) to ensure that it remains necessary and privacy intrusion is justified and proportionate.