SURVEILLANCE CAMERA COMMISSIONER

DATA PROTECTION IMPACT ASSESSMENT

CARRYING OUT A DATA PROTECTION IMPACT ASSESSMENT ON SURVEILLANCE CAMERA SYSTEMS

Purpose of this advice and template

Principle 2 of the surveillance camera code of practice[1] 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 carrying out a data protection impact assessment (DPIA) before any surveillance camera system is installed, whenever a new technology or functionality is being added on to an existing system, or whenever there are plans to process more sensitive data or capture images from a different location. This will assist in assessing and mitigating any privacy issues linked to the use of a surveillance system.

A DPIA is one of the ways that a data controller can check and demonstrate that their processing of personal data is compliant with the General Data Protection Regulation (GDPR)[2] and the Data Protection Act (DPA) 2018. There are statutory requirements to carry out a DPIA in Section 64 DPA 2018 and article 35 of the GDPR.

The Information Commissioner has responsibility for regulating and enforcing data protection law, and has published detailed general guidance on how to approach your data protection impact assessment. In many cases under data protection law, a DPIA is a mandatory requirement. The Surveillance Camera Commissioner (SCC) and the Information Commissioner's Office (ICO) has worked together on this advice, which is tailored to the processing of personal data by surveillance camera systems.

Suggested steps involved in carrying out a DPIA are shown in **Appendix One.**

A further benefit of carrying out a DPIA using this template is that it will help to address statutory requirements under the Human Rights Act 1998 (HRA). Section 6(1) 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 (ECHR). Therefore, in addition to the above, as a public body or any other body that performs public functions you must make sure that your system complies with HRA requirements. Whilst the particular human rights concerns associated with surveillance tend to be those arising from Article 8 which sets out a right to respect for privacy, surveillance does also have the potential to interfere with rights granted under other Articles of the ECHR such as conscience and religion (Article 9), expression (Article 10) or association (Article 11).

If you identify a high risk to privacy that you cannot mitigate adequately, data protection law requires that you must consult the ICO before starting to process personal data. Use of any surveillance camera system with biometric capabilities, such as Automated Facial Recognition technology, is always likely to result in a high risk to the rights and freedoms of individuals and therefore a DPIA must always be carried out in respect of those systems before you process any personal data. There is a risk matrix at **Appendix Two** that can help you to identify these risks.

Who is this template for?

To complement the ICO's detailed general guidance for DPIAs, the SCC has worked with the ICO to prepare this template specifically for those organisations in England and Wales that must have regard to the Surveillance Camera Code of Practice under Section 33(5) of the Protection of Freedoms Act 2012. This template helps such organisations to address their data protection and human rights obligations in the specific context of operating surveillance cameras.

This surveillance camera specific DPIA is also intended to be of value to the wider community of public authorities and any other bodies, whether public or private, who perform public functions. This secondary audience is subject to the same legal obligations under data protection and human rights legislation, and

---

[1] Surveillance Camera Code of Practice issued by the Home Secretary in June 2013 under Section 30(1)(a) Protection of Freedoms Act 2012

[2] Regulation (EU) 2016/679 of the European Parliament and European Council, also known as the General Data Protection Regulation, was transposed into UK law through the Data Protection Act 2018. Any processing of personal data by competent authorities for the prevention, investigation, detection or prosecution of criminal offences is regulated under Part 3 of the Data Protection Act 2018 which transposes Directive (EU) 2016/680, also known as the Law Enforcement Directive, into UK law.

is encouraged by the SCC to follow guidance in the Surveillance Camera Code of Practice on a voluntary basis.

When should you carry out the DPIA process for a surveillance camera system?

- Before any system is installed.
- Whenever a new technology or functionality is being added on to an existing system.
- Whenever there are plans to process more sensitive data or capture images from a different location.

In deciding whether to carry out a DPIA and its scope, consideration must be given to the nature and scope of the surveillance camera activities and their potential to interfere with the privacy rights of individuals.

You **must** carry out a DPIA for any processing of surveillance camera data that is likely to result in a high risk to individual privacy. The GDPR states that a DPIA "shall in particular be required in the case of ……. systematic monitoring of publicly accessible places on a large scale" (Article 35).

Furthermore, as a controller in relation to the processing of personal data, you must seek the advice of a designated Data Protection Officer when carrying out a DPIA.

To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. It is important to embed DPIAs into your organisational processes such as project planning and other management and review activities, and ensure the outcome can influence your plans. A DPIA is not a one-off exercise and you should see it as an ongoing process, and regularly review it.

As part of an ongoing process, your DPIA should be updated whenever you review your surveillance camera systems, it is good practice to do so at least annually, and whenever you are considering introducing new technology or functionality connected to them.

The situations when a DPIA should be carried out, include the following:

- 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 facial recognition, automatic number plate recognition (ANPR), audio recording, 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. Both the Surveillance Camera Code of Practice and the ICO recommend that you review your system annually.
- 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.

If you decide that a DPIA is not necessary for your surveillance camera system, then you must record your decision together with the supporting rationale for your decision.

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(s) the surveillance camera system is trying to resolve.
- Why a surveillance camera system is considered to be part of the most effective solution.
- 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 the lawful basis for surveillance, the necessity of mitigating the problem, the proportionality of any solution, and the governance and accountability arrangements for any surveillance camera system and the data it processes.

The following questions must be considered as part of a DPIA:

- Do you have a lawful basis for any surveillance activity?
- Is the surveillance activity necessary to address a pressing need, for example: public safety; the prevention, investigation, detection or prosecution of criminal offences; or, national security?
- Is surveillance proportionate to the problem that it is designed to mitigate?

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, where your initial answers to these questions can also be recorded.

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

Statutory requirements in Section 64 DPA 2018 and article 35 of the GDPR are that your DPIA **must**:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

Statutory requirements in Sections 69-71 DPA 2018 and articles 37-39 of the GDPR are that if you are a public authority, or if you carry out certain types of processing activities, you **must** designate a Data Protection Officer (DPO) and always seek their advice when carrying out a DPIA. The ICO provides guidance on the requirement to appoint a DPO. If you decide that you don't need to appoint a DPO you should record your decision and your supporting rationale. In the performance of their role, a DPO must report to the highest management level within the controller.

These statutory requirements indicate that a DPIA should be reviewed and signed off at the highest level of governance within an organisation.

To help you follow these requirements this template comprises two parts.

Level One considers the general details of the surveillance camera system and supporting business processes, including any use of integrated surveillance technologies such as automatic facial recognition. It is supported by **Appendix Three** which helps to capture detail when describing the information flows. The SCC's Passport to Compliance provides detailed guidance on identifying your lawful basis for surveillance, approach to consultation, transparency and so on.

Level Two considers the specific implications for the installation and use of each camera and the functionality of the system.

Template – Level One

Location of surveillance camera system being assessed:

Croydon Public Space CCTV System Formed of 94 Networked and 10 Mobile Cameras.

Date of assessment	01/06/2019
Review date	31/05/2020
Name of person responsible	David Eastoe – CCTV & Intelligence Hub Manager
Name of Data Protection Officer	Sandra Herbert – Head of Corporate Law

GDPR and Data Protection Act 2018 and Surveillance Camera Code of Practice

1. What are the problems that you need to address in defining your purpose for using the surveillance camera system? Evidence should be provided which includes 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.

- Deterring crime and assist in the detection of criminal offences
- Deterring anti-social behaviour and assist in the detection of anti-social behaviour incidents
- Reducing the fear of crime and anti-social behaviour
- Improving the safety and security of residents, visitors and the business community who use the facilities covered by the CCTV scheme.
- Assisting the emergency services in the location of Missing Vulnerable persons.

2. Can surveillance camera technology realistically mitigate the risks attached to those problems? State why the use of surveillance cameras can mitigate the risks in practice, including evidence to justify why that would be likely to be the case.

A Public Space CCTV system that is maintained and operated to a high standard is a proven tool in detection and identification of the perpetrators of anti-social behaviour and crime. CCTV cameras within the borough of Croydon are used to enhance public safety and reduce the fear of crime. CCTV can also reduce the time and cost on law enforcement investigating allegations of crime by providing high quality Primary and Secondary evidence for all that require it. Croydon “Town Centres” are particular locations that are a hot spot for crime and Anti-Social Behaviour causing residents and visitors to the borough considerable concern when using their local shops/amenities.

3. What other less privacy-intrusive solutions such as improved lighting have been considered? There is a 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 24/7? Where these types of restrictions have been considered, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

As the Installation of CCTV is often cost prohibitive a joint working group of interested parties such as the Neighbourhood Safety, Anti-Social Behaviour Team, Environmental Response, Environmental Enforcement teams along with Police and Highways colleagues are consulted with a view of considering Non CCTV interventions such as changing the landscape, improved lighting, gates and other such barriers. If CCTV is considered the only solution than a Data Privacy Impact Assessment will be undertaken before any decision is made to install a CCTV camera.

4. What is the lawful basis for using the surveillance camera system? State which lawful basis for processing set out in Article 6 of the GDPR or under Part 3 of DPA 2018 applies when you process the personal data that will be captured through your surveillance camera system.

The introduction of the Section 7 of the Crime and Disorder Act 1998 placed a direct responsibility on local authorities to combat crime and anti-social behaviour. This provides a statutory framework enabling local authorities to consider how their services could contribute to reducing crime and disorder, as well as their impact on social and community factors against that affect crime levels. The Council's CCTV Service supports Croydon Councils corporate priorities to make the Borough Safe, Caring, Healthy, Vibrant, Thriving, Green and Attractive for residents and businesses alike.

Where the allegation relates to a civil offence this information will be processed in accordance with the requirements of the General Data Protection Regulations (GDPR) as amended by DPA18.

DPA 2018, Part 3 – Allows Croydon Council to act as a competent authority (where it has the powers to do so) to process personal data including Special Category Information for the prevention, investigation, detection or prosecution of criminal offences. To use the information in this way the Council must have the powers to enforce the criminal law to process the information and the processing must be necessary and proportionate to that purpose. Personal data can be processed for further related purposes, but no processing must be carried out on it that is incompatible with the initial processing purpose.

The Law Enforcement Directive (LED) enables the Council to process personal information without some of the normal safeguards required by the General Data Protection Regulations. LED controls the processing of personal data were it relates to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to public security.
The Council also uses CCTV camera systems under Section 163 Criminal Justice and Public Order Act 1994.

5. Can you describe the information flows? State how data will be captured, whether it will include audio data, the form of transmission, if there is live monitoring or whether data will be recorded, whether any integrated surveillance technologies such as automatic facial recognition is used, if there is auto deletion after the retention period, written procedures for retention in line with stated purpose, written procedures for sharing data with an approved third party, record keeping requirements, cyber security arrangements and what induction and ongoing training is provided to operating staff. Specific template questions to assist in this description are included in **Appendix Three**.

Networked Public Space Cameras

The Video footage is captured by the camera and transmitted via the BT Fibre network to the VMS (Video Management System) hosting server that is password protected and is situated within the locked equipment room at the Intelligence Hub based in Strand House. No analytical hardware or software is used in conjunction with the Croydon Public Space CCTV cameras.

The stored footage has a retention period of 31 days, after which the VMS automatically overwrites the footage thus deleting it. If the footage is deemed to be of evidential value this can be quarantined by Intelligence Hub Staff for a maximum period of 38 days from the date of initial recording. This is deemed by the Council to be sufficient time for Enforcement Officers (Including the Police) to carry out their investigations diligently. All quarantined footage will be deleted unconditionally after 38 days from initial recording by the CCTV & Intelligence Hub Manager or his/her deputy. Once any quarantined footage has been disclosed to Enforcement Officers (Including the Police), it will be deleted as part of the disclosure process.

Mobile Cameras

The Video footage is captured by the integral camera and stored on to an internal password protected and encrypted hard drive. At the same time a 'live' view is sent via encrypted data stream via the 4G network to a hosting server that is password protected and I situated within the locked equipment room at the Intelligence Hub based in Strand House. No analytical hardware or software is used in conjunction with the mobile cameras. Monitoring by officer within the Intelligence Hub is on an adhoc basis. Access to view and download recorded images can be initiated as required by Intelligence Hub staff by entering a password into the camera interface.

General

The stated purposes and the data retention periods of the Croydon Council Public Space CCTV system can be found in the Croydon Council Public Space CCTV Operations Policy. Procedures for the release of data for enforcement purposes can be found in the Croydon Council CCTV Control Room Manual.

6. What are the views of those who will be under surveillance? Please outline the main comments from the public resulting from your consultation – as part of a DPIA, the data controller should seek the views of those subjects who are likely to come under surveillance or their representatives on the proposition, without prejudice to the protection of commercial or public interests or the security of processing operations. This can often be achieved by existing local consultation mechanisms such as local area committees or safer neighbourhood team meetings; but, if necessary depending on the privacy intrusion of the surveillance in question, other methods could be considered such as face to face interviews, online surveys, questionnaires being sent to residents/businesses and addressing focus groups, crime & disorder partnerships and community forums. The Data Protection Officer may be able to offer advice on how to carry out consultation.

Obviously a number of residents have legitimate concerns regarding the use to which CCTV is put. By ensuring compliance with current legislation we hope to show that the CCTV camera system is only used for the detection and reduction of crime and activities that ultimately assist the public. We have not received any complaints regarding the use of CCTV. Operating staff have been thanked by Partner Agencies and some have received awards for their work. The community is engaged via various ward panels with strong support from elected councillors when Public Space CCTV is discussed. The Council will seek the views of residents regarding the use of Public Space CCTV as part of future engagement and will publish the findings.

7. 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 deployment of an overt CCTV system will achieve this through providing high-quality evidence of those involved and may deter some of those involved now from participating in the future.

It is anticipated that the camera will also provide some reassurance for local residents and reduce their anxiety about crime.

8. What are the privacy risks arising from this surveillance camera system? State the main privacy risks relating to this particular system. For example, who is being recorded; will it only be subjects of interests? 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? What is your assessment of both the likelihood and the severity of any impact on individuals?

The privacy risks and solutions can be summarised as:-

Personal data retained for longer than necessary or personal data collected and stored unnecessarily – video images will be retained for 31 days unless the authority is notified before deletion that they are required by: a data subject, insurance company, the police or other investigation agency.

Disclosure of personal data to unauthorised persons or agencies – Croydon Council will only release footage where it is permitted to do so to law enforcement agencies, and those other agencies that have a lawful reason to be provided with access to the images. Legitimate access to recorded images is set out in the Croydon Council CCTV Operations Policy and Procedural Manual and all Intelligence Hub staff are trained in them before they are allowed to work in the Control Room. The Control Room Command & Control equipment maintains a log of all access to and download of recorded images, which is audited monthly and can be interogated by the CCTV & Intelligence Manager as required. The Council will never release CCTV footage for entertainment purposes.

Intrusive surveillance disproportionate - Due to the nature of CCTV in Town Centre and public areas there will always be a level of collateral intrusion. When necessary other subjects in the footage will have their identity obscured to maintain their privacy. The DPIA cosiders the option for less intrusive means for achieving the same or a similar aim but none available will meet the requirements set out above.

Lack of public support for intrusive (CCTV) surveillance - The community is engaged via various ward panels and Neighbourhood Watch organisation. There is strong support from elected councillors who represent and express the views of the residents of Croydon for the continued use and extension of CCTV cameras in the borough. The Metropolitan Police service makes daily requests for assistance and consider the deployment of CCTV cameras the best means for gathering evidence of offences and ofenders.

Unauthorised third party access to images - the CCTV equipment, cameras and review and control equipment are password protected which markedly reduces the risk of unauthorised access. Members of the public can submit a right of access request and view or receive footage of themselves, in accordance with their rights; this is an important part of the necessary checks and balances to ensure that the use of the CCTV system is proportionate.

9. Have any data protection by design and default features been adopted to reduce privacy intrusion? Could any features be introduced as enhancements? State the privacy enhancing techniques 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 masking on cameras that overlook residential properties? If these have not been adopted, provide a reason.

Access to the recorded images via the Command & Control system at the Intelligence Hub is protected by a user name and password which is allocated by the CCTV Manager with the appropriate level of system access. Access to the control room is restricted to authorised persons only.

Police use of the Control Room facilities which fall outside of RIPA 2000 guidelines will be documented on a form designed by the Council with the agreement of the Local Policing Team. These will be securely stored and will be available for inspection by the Investigatory Powers Commissioner's Office

Privacy zones will be introduced to the camera if there is a risk that it will overlook private premises.

Live images are not encrypted prior to transmission. This would be possible is the camera unit was upgraded markedly to has sufficient computing power to do so, but this is not considered to be a practical option to pursue.

10. What organisations will be using the surveillance camera images, and where is the controller responsibility under the GDPR and Data Protection Act 2018? List the organisation(s) that will use the data derived from the camera system and identify their responsibilities, giving the name of the data controller(s) and any data processors. Specify any data sharing agreements you have with these organisations.

David Eastoe - CCTV & Intelligence Manager - London Borough of Croydon - Data Controller & Processor.

The Metropolitan Police Service is the principal agency that will make use of the recorded images for the investigation of offences.

It is possible to other statutory investigation agencies will also make use of the images such as Croydon Council enforcement services and central government agencies.

Enforcement or Police Officer removing footage from Intelligence Hub - Data Controller

11. Do the images need to be able to recognise or identify individuals, or could the purpose be met using images in which individuals cannot be identified? Explain why images that can recognise or identify people are necessary in practice. For example, cameras deployed for the purpose of ensuring traffic flows freely in a town centre may not need to be capable of capturing images of identifiable individuals, whereas cameras justified on the basis of dealing with problems reflected in assessments showing the current crime hotspots may need to capture images in which individuals can be identified.

It is of paramount importance that the system is capable of identifying individuals as footage from the system will be used in court. If individuals are not identifiable then the system would not be fit for purpose.

12. How will you inform people that they are under surveillance and respond to any Subject Access Requests, the exercise of any other rights of data subjects, complaints or requests for information? State what privacy notices will be made available and your approach to making more detailed information available about your surveillance camera system and the images it processes. In addition, 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:-

- Developed a CCTV Operations Policy that describes in detail who has responsibility and accountability for all Public Space surveillance camera system activities including images and information collected, held and used.

- Published the locations of its Public Space CCTV cameras including mobile cameras and other information relating to the Public Space CCTV system on its Corporate Website at the following address https://www.croydon.gov.uk/community/safercroydon/Services/cctv

- A consistent CCTV signage policy. All areas where CCTV is in use will have clear, consistent signs exhibited to comply with the Data Protection Act; this is to advise people that they are about to enter an area covered by CCTV cameras or to remind them that they are still in an area covered by CCTV. The signs will also act as an additional deterrent. CCTV signs will not be displayed in areas, which do not have CCTV cameras. Signs will carry the outline of a CCTV camera. The information on the sign will explain why the CCTV cameras are there, including Traffic Enforcement purposes, who runs them (London Borough of Croydon) and a contact number (020 8726 6000). The signs, position and the message will be large enough to enable people to easily read the information on it.

- Recognises that individuals whose information is recorded have a right to be provided with that information or, if they consent to it, view that information. Requests will be dealt with promptly. It should be noted that Individuals will only have 31 days to make a request before the footage is automatically deleted. All requests are subject to operational considerations for example where;

    - Footage has been requested by and/or passed to the Police as part of an investigation of a crime; or
    - Footage has been requested in respect of a road traffic collision and the information has been passed to insurers; or
    - Any relevant exemptions that might be considered to apply in respect of the Data Protection Act 1998.

- A Corporate complaints procedure that can be used for any complaints received regarding CCTV operations. Anyone wishing to make comments or observations about the CCTV system should write or email the CCTV & Intelligence Hub Manager whose contact details can be found in the Public Space CCTV Policy.

All of the above is contained on London Borough of Croydon's Website https://www.croydon.gov.uk/community/safercroydon/Services/cctv or by telephoning 020 8726 6000.

13. How will you know if the particular camera system/hardware/software/firmware being considered does deliver the desired benefits now and in the future? It is good practice to review the continued use of your system on a regular basis, at least annually, to ensure it remains necessary, proportionate and effective in meeting its stated purpose. State how the system will continue to meet current and future needs, including your review policy and how you will ensure that your system and procedures are up to date in mitigating the risks linked to the problem.

The Council has purchased a Command, Control & Video Management system from a recognised manufacturer in this field. The systems software is updated on a bi-annual basis and its hardware is assessed on an annual basis to confirm that it is still fit for purpose. The Council will update it CCTV Operations Policy and Control Room manual at least annually to keep up to date with changes in legislation and good working practices. The Council are members of the London CCTV Managers group and the national CCTV Users Group where best practice policies are discussed and disseminated. All camera hardware that is purchased is done so on the basis that it will have a life of at least 7 years and is able to have its firmware updated to allow for changes in operational protocols etc.

14. 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 system will be processed for any other purpose or with additional technical factors (e.g. face identification, traffic monitoring or enforcement, automatic number plate recognition, body worn cameras) in future and how such possibilities will be addressed. Will the camera system have a future dual function or dual purpose?

Legislation can and does change. The Council will comply with all future regulations placed upon it. As populations increase, it is realistic to assume that pressures will be put on Croydon Council to release images to wider audiences. These include other emergency services, solicitors, insurance companies and law enforcement. The Council will have to consider the use of analytical hardware and software such as body language, facial and vehicle number plate recognition. The decision for this will made on a pressing need basis and the benefit of using these technologies to the Council.

15. Have you considered the extent to which your surveillance camera system may interfere with the rights and freedoms conferred under the European Convention on Human Rights? When we consider data protection, our focus tends to be upon the potential to interfere with the Article 8 right to respect for private and family life. Surveillance undertaken in accordance with the law could, however, interfere with other rights and freedoms such as those of conscience and religion (Article 9), expression (Article 10) or association (Article 11). Summarise your assessment of the extent to which you might interfere with ECHR rights and freedoms, and what measures you need to take to ensure that any interference is necessary and proportionate.

The deployment of the Croydon Council Public Space CCTV system is not considered likely to have a negative impact on the rights and freedoms of people as conferred by the ECHR. The use of CCTV is considered to be proportionate and the surveillance will be no more intrusive than necessary to achieve its operational requirement to detect and investigate Crime & ASB in the area surveilled.

The use of the Councils Public Space CCTV system for Covert Directed Surveillance by Law Enforcement and other entitled partners is in strict accordance with the Regulation of Investigatory Powers Act 2000 (RIPA). All such surveillance will only permitted by the Council if it is satisfied that it is warranted and proportionate.

Croydon Council will not use its CCTV cameras to surveil people's homes, cameras are deployed for a specific purpose, the detection & reduction of Crime & ASB and will not be used for the surveillance of members of the public who are going about their daily business. As such, its use will not interfere with people's rights and freedoms under Articles 9, 10 or 11, as described above.

All control room operators have been trained to BTEC Level 2 and are aware of their responsibilities with regard to privacy restrictions on the scope and use of public area CCTV surveillance.

16. Do any of these measures discriminate against any particular sections of the community? Article 14 of the ECHR prohibits discrimination with respect to rights under the Convention. 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.

Croydon Council considers there will be no discriminatory or disproportionate impact on any section of the community arising from the installation of the Croydon Council Public Space CCTV system.

Template Level Two

This Level 2 template is designed to give organisations a simple and easy to use format for recording camera locations, other hardware, software and firmware on their surveillance camera system, and demonstrating an assessment of risk to privacy across their system and the steps taken to mitigate that risk.

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 2012 and/or the Data Protection Act 2018.

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 DPIA should help identify any cameras (irrespective of the type) that may be directed at a more vulnerable area (e.g. a children's play area) and thus presenting a higher privacy risk. This approach allows the organisation to document a generic and methodical approach to any 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. It also allows you to consider the risks associated with any integrated surveillance technology such as automatic facial recognition systems, along with security measures against cyber disruption of your system,

As an organisation that operates a surveillance camera system you will also be the controller of the personal data captured by its cameras. Under DPA 2018 (Sections 69-71), a data controller is under a legal obligation to designate and resource a data protection officer and to seek their advice when carrying out a DPIA.

An example of a risk assessment matrix is shown in **Appendix Two**.

When undertaking a DPIA, it is essential to be able to confirm where the organisation's cameras are sited. It is good practice for all organisations to maintain an asset register for all of their hardware (including cameras), software and firmware. This allows the system operator to record each site and system component in a manner to lead into the level two process.

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

Overall step one and step two will cover the uses of hardware, software and firmware of the system. However, it may be contrary to the purpose of your surveillance camera system to publically list or categorise each individual asset.

Template – Level Two

Step 1 (definition of hardware, software and firmware including 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 camera ability or system functionality due to upgrade.

ID	Camera types	Makes and models used	Amount	Description	Justification and expected use
1	Standard Shoe Box PTZ	Various Components assembled to form complete camera.	61	Colour, Pan, Tilt & Zoom. Standard definition. No Audio Capability	Public space monitoring from CCTV Control Room 24 hours a day 365 days a year.
2	Standard Dome PTZ	Dennard Speed Dome	2	Colour, Pan, Tilt & Zoom. High definition. No Audio Capability	Public space monitoring from CCTV Control Room 24 hours a day 365 days a year.
3	Mini Dome PTZ	HIKVISION Dark Fighter Bosch MIC 5000/7000 Bosch G3 & G4	15	Colour, Pan, Tilt & Zoom. Standard definition. No Audio Capability	Public space monitoring from CCTV Control Room 24 hours a day 365 days a year.
4	Mobile Camera	Vemotion Pole Mini	10	Colour, Pan, Tilt & Zoom. High definition. No Audio Capability	Public space monitoring from CCTV Control Room 24 hours a day 365 days a year.

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.

CAT	Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
A	Residential Street	Standard Shoe Box PTZ Standard Dome PTZ Mini Dome PTZ Mobile Mini Dome PTZ	5	24/365	24 Hours – regular camera patrols based upon risk and intelligence information. 1 Camera Patrolled during 'School Run Only'	Camera has been installed to monitor traffic flow and to allow parking enforcement near local school. Where a camera overlooks a residential property integral camera privacy zones have been installed. CCTV areas have appropriate signage stating its use and purpose with our contact details. All recordings are encrypted and can only be downloaded by trained staff.
B	Town Centre Shopping Areas Local High Streets	Standard Shoe Box PTZ Standard Dome PTZ Mini Dome PTZ Mobile Mini Dome PTZ	56	24/365	24 Hours – regular camera patrols based upon risk and intelligence information.	The privacy expectations in Public Areas of a Town Centre and High Street setting are low. Areas where we have installed CCTV are well signed with appropriate signage stating its use and purpose with our contact details. All recordings are encrypted and can only be downloaded by trained staff.
C	Combined Residential Housing Area with	Standard Shoe Box PTZ	29	24/365	24 Hours – regular camera patrols based upon risk and	The privacy expectations in a Residential street are much higher than in

CAT	Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
	Integral or local Shopping Areas	Standard Dome PTZ Mini Dome PTZ Mobile Mini Dome PTZ			intelligence information.	Public Areas of a Town Centre and High Streets. Cameras are only sited to counter a specific problem. Where a camera overlooks a residential property integral camera privacy zones have been installed. CCTV areas have appropriate signage stating its use and purpose with our contact details. All recordings are encrypted and can only be downloaded by trained staff.
D	External Retail External Leisure Parks External Industrial Parks	Standard Shoe Box PTZ Standard Dome PTZ Mini Dome PTZ Mobile Mini Dome PTZ	4	24/365	24 Hours – regular camera patrols based upon risk and intelligence information.	Privacy expectations around Retail, Leisure and Business Parks are similar to the Town Centre and High Street settings and are low. Areas where we have installed CCTV are well signed with appropriate signage stating its use and purpose with our contact details. All recordings are encrypted and can only be downloaded by trained staff.

Step 3 (Cameras or functionality where additional mitigation required)

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

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

Asset No	Camera Type	Location Category	Further Mitigation/Comments (Optional)
350	3	C	
352	1	B	
353	3	B	
400	3	C	
401	3	C	
402	3	C	
403	3	C	
404	3	C	
405	3	C	
406	3	C	
425	1	B	
426	3	B	
428	1	B	
450	1	B	
452	1	B	
454	3	B	
798	3	B	
799	3	B	
801	1	C	
802	1	C	
803	1	C	
804	3	C	
805	1	C	
806	1	C	
807	1	C	
808	3	C	
809	1	C	
820	1	B	
821	3	B	
822	1	B	
823	1	B	
824	1	B	
825	1	B	
826	1	C	
827	1	C	
828	1	C	

829	1	C	
830	1	C	
831	1	C	
832	1	C	
833	1	C	
834	1	B	
835	1	B	
836	1	B	
837	1	B	
838	3	A	
839	3	A	
840	3	A	
841	3	A	
842	3	A	
850	3	C	
851	1	B	
852	3	D	
853	3	D	
855	3	D	
856	3	D	
857	3	C	
860	1	B	
861	1	C	
862	1	B	
863	1	B	
864	1	B	
865	3	B	
870	1	B	
871	1	B	
872	2	B	
877	1	B	
879	3	C	
880	1	C	
882	3	B	
883	3	B	
884	1	B	
885	3	B	
886	2	B	
887	1	B	
888	3	B	
889	3	B	
890	1	B	
891	1	B	
892	1	B	
893	1	B	

894	1	B	
895	1	B	
896	1	B	
898	3	B	
899	3	B	
900	3	B	
901	3	B	
902	3	B	
903	3	B	
904	3	B	
905	3	B	
906	3	B	
907	3	B	
9001	4	A,B,C & D	
9002	4	A,B,C & D	
9003	4	A,B,C & D	
9004	4	A,B,C & D	
9005	4	A,B,C & D	
9006	4	A,B,C & D	
9007	4	A,B,C & D	
9008	4	A,B,C & D	
9009	4	A,B,C & D	
9010	4	A,B,C & D	

Step 4 (Mitigation for specific cameras and any integrated surveillance functionality that have high privacy risks)

Where there is a very high risk to privacy you may wish to conduct an extensive DPIA of specific installations or functionality and have it fully documented. Where you are unable to mitigate the risk adequately you **must** refer your DPIA to the ICO for review.

DPIA for specific installations or functionality

Camera number	Not Applicable
Camera location	Not Applicable

Privacy risk(s)	**Solution**	**Outcome** (Is the risk removed, reduced or accepted)	**Justification** (Is the impact after implementing each solution justified, compliant and proportionate to the aim of the camera?)

Measures approved by:
Integrate actions back into project plan, with date and responsibility for completion

Name	David Eastoe
Date	01/04/2019

Residual risks approved by:
If you identify a high risk that you cannot mitigate adequately, you must consult the ICO before starting to capture and process images

Name	Not Applicable
Date	

DPO advice provided:
DPO should advise on compliance and whether processing can proceed

Name	Sandra Herbert
Date	01/04/2019
Summary of DPO advice	Processing can proceed

DPO advice accepted or overruled by:
If overruled, you must explain your reasons

Name	David Eastoe
Date	
Comments	

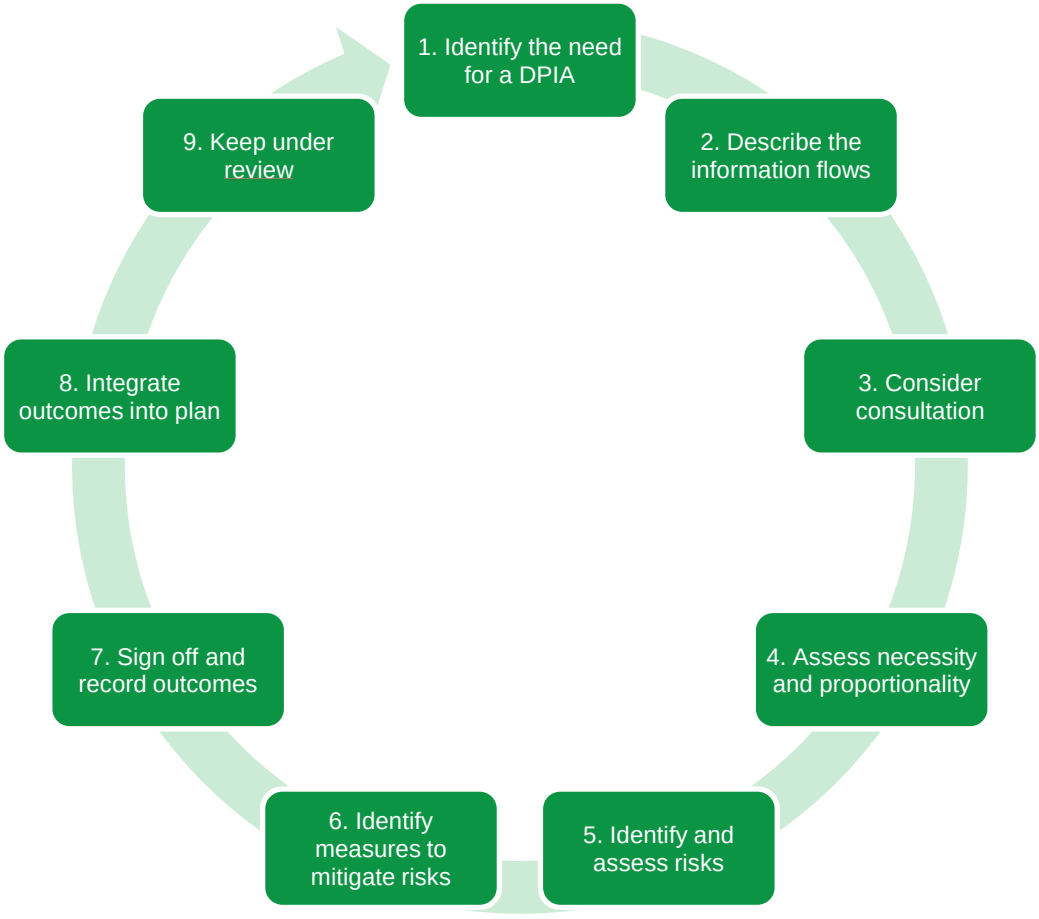
Consultation responses reviewed by:
If your decision departs from individuals' views, you must explain your reasons

Name	
Date	
Comments	

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

Name	David Eastoe
Date	

APPENDIX ONE: STEPS IN CARRYING OUT A DPIA



APPENDIX TWO: DATA PROTECTION RISK ASSESSMENT MATRIX

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

Matrix Example:

	Location	Camera Types			
		Standard Shoe Box PTZ	Mini Dome PTZ	Midi Dome PTZ	Mobile Camera
Low Impact ↓ High Impact	Town Centre Shopping Areas Local High Streets	1B	2B	3B	4B
	External Retail Parks External Leisure Parks External Industrial Parks	1D	2D	3D	4D
	Combined Residential Housing Area with Integral or local Shopping Areas	1C	2C	3C	4C
	Residential Street	1A	2A	3A	4A

Low Impact	Medium Impact	High Impact	

Be aware that use of any surveillance camera system with biometric capabilities, such as Automated Facial Recognition technology, is always likely to result in a high risk to the rights and freedoms of individuals and therefore a DPIA must always be carried out in respect of those systems before you process any personal data.

APPENDIX THREE: LEVEL 1

DESCRIBE THE INFORMATION FLOWS

Optional questions to help describe the collection, use and deletion of personal data.

It may also be useful to refer to a flow diagram or another way of explaining data flows.

5.1 How is information collected?

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

5.2 Does the system's 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), and whether it also enables audio recording.

Networked Camera Images recorded at Council CCTV Control Room.
Mobile Cameras recorded on local encrypted hard drive.
Cameras not audio capable.

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 control room is a secure area and access is restricted to members of Control Room staff via combined Identity and access control card. Access to others is controlled via Control Room staff.

Access to the recorded images in the control room is restricted to authorised persons via user name and password. Permissions are granted by CCTV & Intellgence Hub Manager.

5.3 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)

4G wireless transmission and images are accessed via CCTV review workstation connected to a broadband service in the control room

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

Analogue Images are transmitted to the Control Room via End to End Fibre transmission circuits provided by BT. Access to transmission equipment is via lock at the camera end and access control at the Control Room end.

5.5 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)

Residential Streets

5.6 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)

5.7 What measures are in place to mitigate the risk of cyber attacks which interrupt service or lead to the unauthorised disclosure of images and information?

Data is Encrypted and Password protected. Passwords are changed from default and changed on a regular basis.

5.8 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 Automatic Facial Recognition software

☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software

☒ Used to search for vulnerable persons

☒ Used to search for wanted persons

☒ Recorded data disclosed to authorised agencies to support post incident investigation by, including law enforcement agencies

☐ Recorded data disclosed to authorised agencies to provide intelligence

☐ Other (please specify)

5.9 How long is footage stored? (Please state retention period)

Data from the networked static cameras is retained for 31 Days.
The footage from the mobile cameras is usually retained for 15 days but this depends on the activity within the cameras range.

5.10 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)

Video images the networked static cameras are deleted automatically after 31 days. Images that are quarantined at the request of Law and other enforcement officers is deleted by the CCTV & Intelligence Manager and Team Leaders 38 days from initial recording unconditionally. The Council believes 38 days allows Law and other enforcement officers sufficient time to collect images if the become aware of the need to collect them near the end of the retention period.

5.11 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)

5.12 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)

Copies not collected by hand are sent via registered post or encrypted email via Egress Switch.

5.13 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)

disclosure, production, accessed, handled, received, stored information

5.14 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)

5.15 Do CCTV operators receive ongoing training?

☒ Yes ☐ No

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

☒ Yes ☐ No