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:

South Kesteven District Council
CCTV Control Room, Mowbeck Way, Grantham
Main Council Building, St Peters Hill, Grantham
Streetcare Services, Mowbeck Way, Grantham
Guidhall Arts Centre Grantham
Stamford Arts Centre
Bourne Customer Access Point

Date of assessment	October 2023
Review date	October 2024
Name of person responsible	Ayeisha Kirkham
Name of Data Protection Officer	Graham Watts

Unknown
25/10/2023, 11:57:21

Ayeisha Kirkham

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

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.

Although there are related benefits in terms of health and safety and asset security the main objectives for the installation and continued use of CCTV with South Kesteven to;
- Assist in the detection and prevention of crime, along with the maintenance of public order by providing evidence.
- Facilitate the apprehension and prosecution of offenders in relation to crime and public order Reduce public disorder and anti social behaviour and enhance the general publics perception of safety.
- Assist in the tracking and apprehension of persons who are suspected of committing a criminal offence.
- Assist in the identification of witnesses.
- Promote the objectives of the Safer Lincolnshire Partnership.
- Provide the Police and the Council with evidence to take criminal and civil action in the courts
- To assist in improving the environment in the areas covered.
- Maintain and enhance the commercial viability of the District and encourage continued investment.

Reported crime figures are reviewed on a monthly basis in order to evaluate crime trends/hot spots and to ensure the requirements and aims of the system remain valid. The reduction in policing numbers within Lincolnshire has also influenced the operational requirements of the CCTV system, it is quite often the case that an immediate police response is not available which results in CCTV evidence being invaluable as this can be used post incident in order to identify offenders.

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.

Public Space CCTV used lawfully and in a proportionate manner is a useful and proven method to reduce the impacts of crime and ASB in our communities. Carefully managed evidence processing continues to be an effective way to assist the Police, Local Authority staff and those who have a statutory role in achieving successful prosecutions. It is also used to assist with major events for public safety, reduce traffic congestion, and improve road safety.

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.

CCTV cameras are not installed by South Kesteven District Council unless other actions have first been either considered, or attempted over a period of time to resolve or reduce the problem. Actions taken will depend on the location, the circumstances of the issue(s), the risk of harm, and the vulnerability and the wishes of victims. Action considered may potentially include; improved lighting, extra police patrols, extra youth outreach patrols, extra security officer patrols, crime prevention and target hardening measures, encouraging public reporting of problems, restorative interventions, and the diversion, support, treatment, and education of perpetrators, along with enforcement actions.
Improved/relocated lighting and other methods to design out crime such as gating off rat runs and removing street furniture are also considered, advice can also be sought from the Police Architectural liason officer should this be necessary. The type and frequency of offences will sometimes lead to the installation of CCTV as this becomes the most effective in terms of costs, quality of evidence, reliability and the proven positive impact it can have. The advances in technology have now made it possible to reduce the numbers of cameras in certain locations and create privacy zones on cameras thereby lessening the intrusion upon privacy.

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.

GDPR Article 6(1) e: processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.
Data Protection Act 2018, Schedule 2, Part 2.
Section 17 of the Crime and Disorder Act 1998, as amended by the Police and Justice Act 2006, requires responsible authorities to consider crime and disorder (including antisocial behaviour and other behaviour adversely affecting the local environment); and the misuse of drugs, alcohol and other substances in the exercise of all their duties, activities and decision-making. This means that in all policies, strategies and service delivery there is a need to consider the likely impact on crime and disorder.

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**.

Data is captured in video format only, this does not include audio. The only surveillance in use with audio is the body worn cameras at the point that an enforcement officer approaches a recipient of a fixed penalty ticket. There is a specific policy in place for such instances in order to reduce the intrusion upon others. The system is hard wired on BT fibre and Council Network, there are no other methods of transmission in use. There is live monitoring from the main control room with some cameras being record only. These can only be reviewed where a need is identified and with confirmation of a lawful basis for processing. The retention periods, procedures, data sharing arrangements and security are in accordance with the councils CCTV code of practice and policies. Authorised staff have received relevant training in legislation, local operating procedures and use of the system. There are no integrated technologies in use such as Automatic Number Plate or Facial Recognition Systems. Auto deletion is set for all recorder images with the retention periods being set according to requirements and in line with the DPA ie kept no longer than is necessary. Information sharing agreements are in place for all relevant partners within the Safer Lincolnshire Partnership, with arrangements and set protocols in place for sharing with others (insurance companies) and private individuals in line with DPA (subject access requests)

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.

The town centre CCTV system has been in place since 1997, this was a joint initiative by the Local Authority, Police and local businesses. Although little documentation is available regarding consultation at that point it is clear from speaking with community representation in terms of elected members that there was great support for the initial scheme and continued support when decisions are being made regarding the installation of further cameras. Consultation is carried out for new installations with the consultation groups, methods and duration being set on a case by case basis. The sensitivity of location and the impacts of possible intrusion would also be considered during the initial planning with alternative crime prevention interventions being considered before the installation of CCTV. Recent consultation regarding a camera installation received only positive comments and support. The consultation was also useful as it allowed us to address privacy concerns raised by one member of the public.
In respect of the workplace internal CCTV, it has been installed to maintain the safety of members of staff, for the prevention and detection of crime and internal management actions. No consultation was conducted as there have been several cases of criminal activity and the installation of the internal CCTV was a direct action as a result of this.

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.

CCTV as a form of evidence is used on a frequent basis and with the regular maintenance of the equipment and operation by trained and Licensed staff, it provides quality primary and secondary evidence for all those authorised to use it. Maintaining reasssurance of the public is paramount if localities are to maintan public confidence and achieve continued financial investement and support from the business sector. The clear and pressing need for the continuation of CCTV within our localities is supported by the year on year increase in certain crime types and the reduction in the resources of other primary agencies such as the Police and Trading Standards. A strong communications strategy along with other interventions such as retail radio schemes, banning orders and other softer initiatives are also important as they sometimes reduce the requirement to further expand CCTV schemes.

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?

Privacy and intrusion are the primary consideration when any new camera location is being considered. The use of technology can and is used to reduce intrusion, such as digital masking of certain locations with operator training and system audits being an important aspect. Data retention schedules and adherence to information sharing agreements is also important as is adequate signage. Procedures are in place to manage the recordings and security of personal data, the retention deletion and access to live images and recorded data, privacy zones and excessive or innapropriate monitoring.

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.

Safeguards are in place to ensure the privacy of data subjects. This includes but is not restricted to; staff training, supervision, the consideration and use of privacy zones and system audits. It is also important to note that cameras should not be over specified, they need to gather the required information and no more,. ie don't install a camera with a 36 zoom capacity if a 24 zoom will suffice. Cameras installed in SKDC owned temporary accommodation properties are located in communal areas only and all tenants are informed and sign to acknowledge their presence and purpose.The cameras are angled to respect privacy.
Staff have been informed about the cameras installed within the Waste Dept building. No audio is recorded and there is no live monitoring. Images are only accessed in response to an incident/event that requires further investigation.
The council will undertake periodic dip testing on all cameras to ensure that the cameras are in suitable working order and there are no faults detected and also to ensure they are viewed to take appropriate internal management actions as necessary.

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.

The Council's Data Protection Officer is responsible for all data held by the Council.

In addition the CCTV monitoring centre staff are also responsible for the security of any data held by the CCTV Centre.

Named members of staff within the Housing Dept are responsible for the security of any data captured via the cameras in SKDC owned temporary accommodation.

Named members of staff within the Stamford Arts Centre are responsible for the security of any data captured by the cameras located at the Stamford Arts Centre.

The following persons/organisations may obtain/use images held by the Council:
(1) Data Subjects - personal use
(2) Police/Transport Police - investigation of offences
(3) Any Statutory or Enforcement Organisation carrying out their statutory, or investigatory, regulatory, licensing, or enforcement duties
(4) Insurance Companies - on behalf of clients involed in civil and criminal cases
(5) Solicitors Chambers - on behalf of clients involved in civil and criminal cases

A Multi Agency Information Sharing Agreement is in place (Safer Lincolnshire Partnership)

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.

Images must be fit for purpose, in this case the primary function is for the prevention and detection of crime. Recorded images must be cabable of producing images of a quality that would allow the identification of individuals who may be suspects or witnesses relating to a criminal offence. This would include clothing and vehicle makes and registration numbers. The same cameras could also be used

to monitor traffic flow but would be positioned to achieve a broader and less intrusive view in order to lessen the impact upon data subjects.

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.

ICO compliant signage is displayed in areas covered by CCTV, officers wearing body worn cameras also wear badges informing the public that video and audi recordings may be taking place. Subject access requests available and evaluated by the Data Protection Officer. Privacy notices and complaint policy published on the Councils website as are the CCTV Code of practice, DPIA, Self Assessment, Camera locations and performance indicators. The tenants of the temporary accommodations are informed and sign to acknowledge the cameras presence and purpose. Members of staff who work within the areas covered by CCTV in the Waste Operations building have been informed of the location and purpose of the cameras.

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 annual system review using the SCC self assessment tool will provide a basis for any system upgrades should they be required. Findings from this review may also require the CCTV code of practice to be updated along with any specific operational requirements. Regular system audits and feedback from control room staff forms an important aspect of system performance supported by a fully comprehensive maintenance contract. Requests for new camera installations are evaluated by the SPoC in conjunction with the DPO and relevant Head of service (Housing, facilities, economic development) and approved camera installation contractor. Camera cleaning schedule and fully comprehensive maintenance contract in place. Membership of the Public CCTV managers association also important in order to maintain knowledge of developments in technology and changes in legislation, informing local policy and development of longer term CCTV strategies.

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?

Any significant deviation fom the current operating requirements will require evaluation and sign off by the SPoC and DPO in conjunction with the CCTV Management group and Elected Member with the responsbility for CCTV.

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 CCTV covers open space, areas where the public have access such as customer contact centres and work areas. Staff and the public are aware that CCTV is recording (adequate signage) The level of expectation regarding privacy is low with the use of CCTV in accordance with the stated objectives deemed to be proportionate and not in conflict with Articles (8),(9),(10),(11) or (14) of the HRA.

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.

No potential for discrimination or disproportionate impact upon any section of the community has been identified during the evaluation phase prior to any recent installations nor has it been identified prior either by council officers, Elected Members, partner agencies or indeed by the public themselves.

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.

Please see example below:

ID	Camera types	Makes and models used	Amount	Description	Justification and expected use
1.	Fixed Internal- Live Feed	Various	41	Fixed view	Crime Prevention/Detection, Public Safety, internal management function
2.	Fixed ExternalLive Feed	Various	27	Fixed view	Crime Prevention/Detection Public space monitoring, ability to monitor live from CCTV control room 24/7
3.	Fixed Internal- Review Only	Various	17	Fixed view	Crime Prevention/Detection, Public Safety, internal management functions
4.	PTZ External- Live Feed	Various	85	Pan, tilt and zoom function	Crime Prevention/Detection Public space monitoring, ability to monitor live from CCTV control room 24/7
5.	Body Worn Video - Review Only	Reveal D Series	3	Fixed lens, fixed view	Evidence of offence and Staff safety. Offence and customer interaction recording
6.	Fixed- Freighters - Review Only	ISS RXSL2/ISSRX3	120	Fixed lens, fixed view	Staff safety, health and safety, compliance with policies/procedures
7.	Fixed - external perimeter of Waste building, within the workshop and on the fuel pumps - Review Only	L-TU-IP5M-2.8-1 fixed turret camera	11	Fixed lens, fixed view	Staff safety, health and safety compliance with policies/procedures, crime prevention, detection/investigation of criminal offences. Privacy expectation is low within the workshop and external areas of the building.

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.	Public Space Town centre Car Parks Residential	1, 2, 4	114	Yes- 24/7 Images retained for 30Days	Yes, 24/7 Hourly patrols carried out	Cameras are installed here to respond to high crime trends, deal with the fear of crime. The privacy level expectation in a town centre is low.
B.	Parks	2, 4	14	Yes- 24/7 Images retained for 30 Days	Yes	Cameras are installed here to protect people, prevention and detection of crime and deal with the fear of crime. The privacy level expectation in parks is low.
C.	Public Buildings Internal- Main System	1, 4	18	Yes- 24/7 Images retained for 14Days	No, images reviewed upon an incident being reported	Cameras are installed here to protect persons and assets. The privacy level expectation is low.
D.	Public Buildings Internal- Stand Alone	3,	13	Yes- 24/7 Images retained for 14Days	No	Cameras are installed here to protect persons and assets. The privacy level expectation is low.
E.	Freighters	6	120	Yes- only when vehicle in use, Images retained for 14Days	No	Compliance with policy, Health and Safety Legislation, protection of our staff and the public
F.	Body Worn	5	3	Yes- Only when activated by an officer	No	Compliance with policy, protection of our staff and the public

CAT	Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
				30Days/6 months for prosecutions		
G.	Fixed external DWO building	2,	6	Images retained for 14 days	Yes	Cameras are installed to protect people and assets. Privacy expectation is low.

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 number	Reviewed	Camera type	Location category	Further mitigation/ comments (optional)
27 and 52	Yvonne Swinton Reviewed October 2021	5	A	Digital masking has been applied in order to remove any possible ability to see into windows of nearby properties.
57	Yvonne Swinton Reviewed April 2022	5	A	Digital masking has been applied following request by occupier of nearby property to prevent any possibility of sight into the property.
206, 207, 208, 209, 210, 211	Yvonne Swinton Reviewed April 2022	5	B	Digital masking has been applied in order to remove any possible ability to see windows of properties overlooking the park area.

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	None identified
Camera location	N/A

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	N\A
Date	

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	N\A
Date	

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

Name	Graham Watts - Data Protection Officer
Date	27/10/2023
Summary of DPO advice	Surveillance is adequate, proportionate and lawful.

Unknown
27/10/2023, 11:58:44

Graham Watts - Data Protection Officer

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

Name	Karen Bradford - Chief Executive
Date	31/10/23
Comments	Advice accepted

Unknown
31/10/2023, 11:59:13

Karen Bradford - Chief Executive

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

Name	N/A
Date	
Comments	

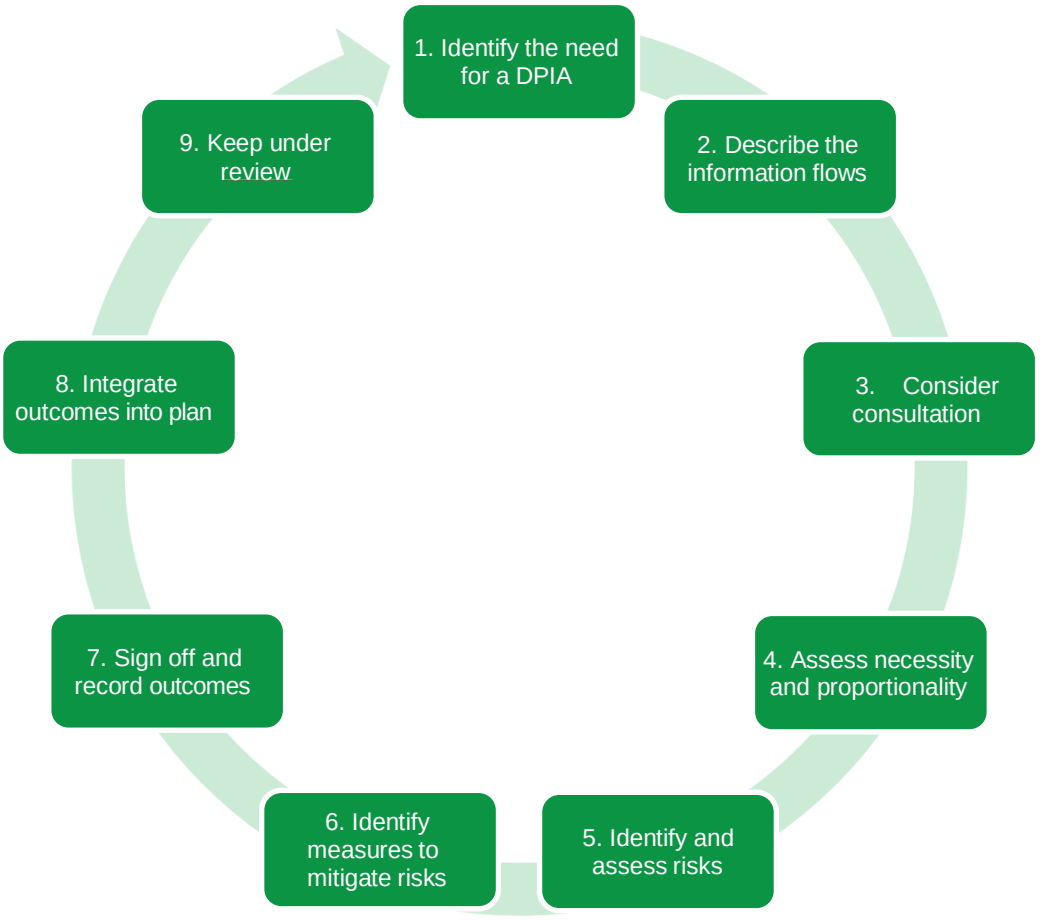
This DPIA will kept under review by:
The DPO should also review ongoing compliance with DPIA

Name	Ayeisha Kirkham - Head of Public Protection
Date	30/10/2023

Unknown
30/10/2023, 11:59:46

Ayeisha Kirkham - Head of Public Protection

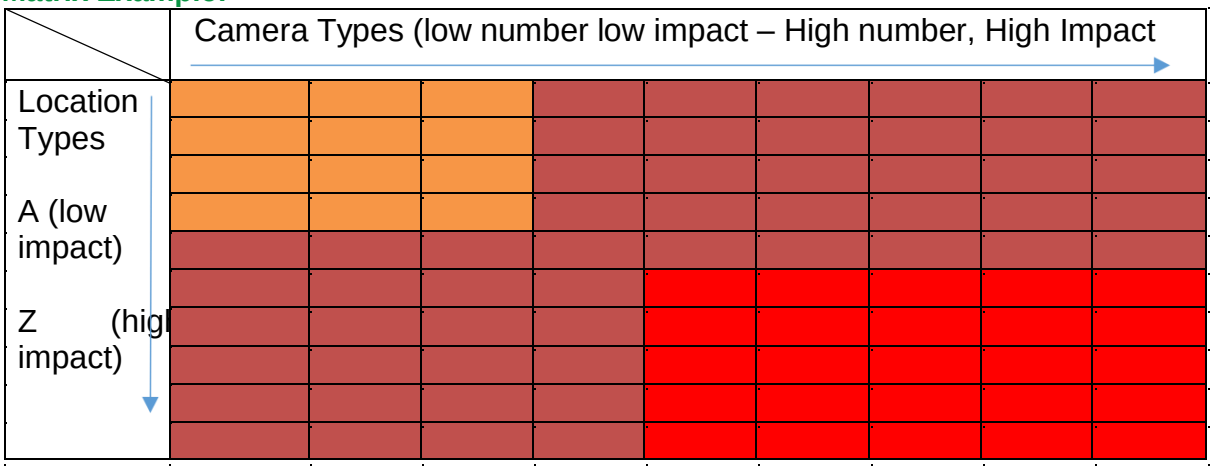
APPENDIX ONE: STEPS IN CARRYING OUT A DPIA



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:



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

Other- Cameras installed waste freighters- primary use being health and safety

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.

Local Authority CCTV Control Room
Freighters
Body Worn Camera- Includes Audio

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)

Yes- Secure control room for Town Centre CCTV recordings and body worn cameras
Password protection and authorised officer to view recorded images for stand alone sites

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

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

Hard wired refers to IP cameras over secure local area network

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

CCTV camera have point to point encryption, password protected and software specific for access. They are VLAN separated on the local network. CCTV is separate from the data and telephony traffic.

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)

Buildings/premises- Internal public areas- Customer Contact Centres, Arts Centres.
Public Spaces, town centres, residential estates, car parks, parks

☒ Other (please specify)

Freighters
Body Worn Video

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)

Vehicle- captured as by product of monitoring incidents- No ANPR or refference database in use
Other- Body Worn Video- images captured when issuing fixed penalty notices

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?

All cameras have wireless ports disabled
Firewalls in place
Ability to carry out penetration testing

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)

Secondary/Bi Product- used to monitor traffic flow and update relevant agencies ie Police, Highways Authority- general overview of areas,

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

Public Space Town Centre - 30 Days
Internal Cameras/Public area - 14 Days
Freighters - 56 Days to allow for information/complaints to be received
Waste Building - 42 Days due to previous criminal activity and the time taken to detect.
Wyndham Park - 30 Days
Body Worn Video- 30 Days to allow for statutory fixed penalty appeal period. 6 months if further prosecution is necessary following expiry of payment period.

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)

In certain circumastances images will be retained for longer than the stated retention period, this is very rare and in relation to an offence where specific timings and locations are unable to initially be varified.

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

☒ Statutory prosecution agencies

☒ Judicial system

☒ Data subjects

☒ Local Government agencies

☒ Legal representatives

☐ Other (please specify)

Judicial System- Via Police

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 of images sent by recored delivery or collected by the data subject upon proof of identity

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)

Information contained within system code of practice and published on Council website
Audit relates to- viewing, production, disclosure, storage, seizure.

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)

Staff will be Licensed and receive all relevant training to achieve this, refresher training also carried out in other aspects such as data protection, RIPA, safeguarding and prevent agenda.

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