DATA PROTECTION IMPACT ASSESSMENT

CARRYING OUT A DATA PROTECTION IMPACT ASSESSMENT ON MOBILE SURVEILLANCE CAMERA SYSTEMS

Date	09/12/19
Location	Ashby Cricket Club Pavillion
Camera	Mobile C1
Request from	Police
Review date	09/02/19

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

---

[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.

audience is subject to the same legal obligations under data protection and human rights legislation, and 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:

Ashby Cricket Club Pavillion Station Road LE652GP

Date of assessment	09/12/19
Review date	09/02/19
Name of person responsible	Paul Collett
Name of Data Protection Officer	Nic~~h~~ola Taylor

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.

Littering, beer bottles and cans and drug use at the Cricket Club. Over a dozen dealer bags. The Cricket Club has become more of a hotspot since the car park at the hotel closed and extra attention to Range Road, The same group have appeared to have gravitated to the cricket club. On attending the location there was a numerous number, over 12 of used 'dealer' bags of drugs and a mass amount of litter, beer bottles and cans. A marked car can access the private road to the cricket club from Station Road; the group hang out on a blind spot to the right of the road in front of the Cricket Club. An individual has been arrested for possession of a class be. Others have been warned. Police are patrolling but have requested a camera. I visitied the location and found significant litter, Damage a small Zip lock bags that smelled of Canabis. The area being misused is hidden and a good site for groups to gather. On discussion with the Victim, he stated that the offendetrs are allso accessing the roof and this is a significant risk. The area has seen a significant increase in the past few weeks and the club are constatly cleaning the area. It is imacting on the club resources. They belive that is now a daily occurance.

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.

We have chosen the deployment following a meeting at the JAG and it was decided that this the best option to address these reports. The location is well placed for for the deployment of the camera, but other measures are being taken. Anti Climb devices will be installed to reduce access to the roof space Police are patroling the area Consideration for detactched youth workers (impact)

The camera will ben used to identify the offenders and enforce via the Incremental approach. There is a belief that this group is known from the work earlier this year at the Royal hotel. The camera will be able to confirm this.

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 describe other option are already in place, but a camera is required. Due to the nature of trhearea, intrustion into privacy is low. This is not a public site and an expextion of privacy is reduces as they are knowingly treaspassing.

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.

To investigate reported criminal behaviour. Our aim is to prevent , detect or deter crime. I believe that this action is lawful as it will be processing information that 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, in this case in our duty to reduce crime and disorder. (Sec 17 CDA98)

GDPR - 6 1 (e) - Performance of a task carried out in the public interest.

DPA 2018 – Schedule 2, Part 1, Paragraph 2 – Prevention or detection of crime

The deployment of this Mobile camera unit is to reduce specific identifed crime type and has been authorised by a panel of intested parties, including Police, fie service, Schools, Legal team, Social care, Community safety team and the OPCC. the task at hand is sepcifically focuesed to deliever a proven need.

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**.

The data is captured on a secure (password protected) and encrypted hardrive using a bespopke operating system. the information is stored on an edge recording device, (hard drive inside the the camera)

Access is via 4G on a Computer stored in a secure facillity. (CCTV control Room) this is manned by SIA badge staff. footage is seized using the council process and meets the criminal standard for Data handling.

The system can produce still images and video, but can not edit the footage beyond cutting video length. Access is restricted to police and council community safety team. It is not shared beyond this.

The footage is only reviewed Post incident and No live monitoring Is undertaked, beyond routine system test (1 per month) to ensure that the unit is functioning and is accurate

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.

This is a reactive deployment and we have NOT consulted. all residents of the property will be informed of the install. the decision to install was made at the Joint Action Group (JAG). Police, Housing, Social care , mental health and others were present. we never consult of mobile deployments. This is not a public site and an exopextion of privacy is reduces as they are knowingly treaspassing.

For all deployment we will post sinage locally with a contact details for comment.

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.

Our aim it to prevent or detect crimes that are affecting the area. The evidence will be used to improve the lives of residents to by preventing and detecting crime. It also shows our commitment to residents and service users by protecting a community asset. The camera will be used to identify the offenders and enforce via the Incremental approach. There is a belief that this group is known from the work earlier this year at the Royal hotel. The camera will be able to confirm this

Prior to deployements a written request from for a member of the Community safety Partnership is required A camera request form must be used. This is debated at JAG and a decision is made as to the best approach. All avenues are explored with a range of tactics suggested. The Camera is only deployed if there is no other options.

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 Locations is a private club site, next to a pubilc bath grounds. The camera will be set to only cover private areas. As we are in the Off season for Cricket, the area is not uin use. The only people accessing the area are either staff or the offenders. We do not see impact on individuals privacy other than enforcement against those offending.

The footage is stored for 30 days. Images and information will be stored in line with industry standards, relevant to the type of CCTV system installed.

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.

The camera securly stores the data and this is encrypted on the hard drive. Even if the unit is stolen the data can't be access without the 8 digit Alphanumerical code and password. The Laptop with this information is secure in an access controlled room (CCTV control).

The Ecyption is 256wep and meet the required standads. The product is secue be design.

Should an SAR be made, The NWLDC process will be followed and logged accordingly.

The ICO has produced a Data Protection Code of Practice for CCTV to assist organisations who use CCTV to comply with the Data Protection Act 20181998. The ICO regulates the Data Protection Act in the UK. The ICO Code of Practice details how CCCTV can be compliant with the 8 guiding principles of the Data Protection Act 20181998. The Code gives guidance in areas such as deciding when CCTV, UAS & BWV should be used, governance of the personal data CCTV system collect, how to use the equipment and organisational responsibilities. As with the SCC Code of Practice, the ICO Code has been adopted, in full, by the Council.

Recorded images and CCTV information will only be used for the purposes defined in this Policy and in line with both the ICO and SCC Codes of Practice. The ownership of the recorded material is with the council as the Data Controller.

Recording equipment will be checked to a regular schedule, as defined in each team operating process.

CCTV, images will only be viewed when there is a legitimate business reason to do so and the showing of recorded material to other internal or external individuals will only be allowed in accordance with the law.

Recorded images must be stored securely in digital format. Where there is a lawful reason to keep an image longer than the usual set retention period the image will be copied and stored securely, again in digital format, with new, relevant set retentions documented. Where relevant the other Council policies will also govern how certain aspects of the council's CCTV, systems are used, like the Information Security & Acceptable Use Policy.

While CCTV, footage can be requested through various routes, predominantly the Data Protection Act 20181998 or the Freedom of Information Act 2000, NWLDC will process all requests from the public or their agents through a single portal to the Council Data Protection Officer. Details of this process will be displayed on the council website and paper form will be available on request. No charge for Subject access requests from individuals will be made, but business will be charged £50 for a Subject Access Requests (SAR) The council retains the right to reject a subject access request, should the request be unlawful or would breach the privacy of others without their consent.

Inappropriate access, use or disclosure of CCTV, footage may put members of the public, employees or CCTV, operators at risk of serious harm, damage or distress. The Council will be at risk of reputational damage and/or be in breach of the law.

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.

All data is the property of NWLDC and we are the Data Controller. The only access granted will be with police under Sec 115 CDA. The data will be processed (Downloaded and saved to a DVD) by control room staff whom are SIA badged. Any data handed to the police will be done in accordance with NWLDC operating process and police guidance for the seizing of evidence. This is all recorded in the control room.all information is signed out of the control room. If seized for evidence, the police take ownership and will dispose of the data once the investigation is complete.

The only partner to access this data will be the police as per described. The police will act as joint data controllers. The Forces Data Officer will be responsible for any information lawfully seized by the Police.

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.

The camera will be set to identify potential offenders and with be in FULL HD at short range. The identification of individual is the aim so the cameras will gather facial details. This is to complete the Specific task for which it has been deployed.

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 Signage used gives clear points of contact.

Our website also hold the privacy statement about our CCTV that the residents can access. Below is the opening state ment for making a subject access request (SAR)

Under the terms of the Data Protection Act 2018, a person is entitled to ask the Council for a copy of all the personal information that it holds about him/her for the purposes of providing services and carrying out its statutory duties and other functions. This includes data held on computers, paper files and closed circuit television systems (CCTV).This form has been designed to assist us in locating your personal information and the more details you can give us concerning the personal information that you are interested in receiving, the quicker we can trace it and provide you with that information. There is a different form for CCTV requests.

The full SAR for CCTV is attached to the bottom o~~g~~f this form.

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 system used is kept up to date and is serviced once a year. the OS is updated on a regular basis by the supplier. It meets our needs and was purchased for a specifed purpose. the OP is current and upto date.

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?

Nil. The only access will be granted to follow up on REPORTED criminal activity.No access for other reasons such as Housing or parking will be granted.

We have a clear polic~~loic~~y in regards to access and we will only use this camera for the specific p~~o~~urpose requested.

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.

Yes. The deployment covers a public open space where the expection of privacy is lower, but is still important. The area under survellence does not cover any sensitive properties. (GP, Hospital, Social care building or solicitor office. No place of worship is captured in this deployment.

Article 8- We never cover private property with a mobile unit unless a RIPA is obtained. If this is the case, then Prior to deployment, the RIPA will be reviewed in person.
Articles 9, 10-not aeffected
Article 11- This may be impacted as groups with the offender may be filmed as well and there is a risk of Guilt by association. This will be considered upon reviewing the footage, as with a regular incident.

The use of this camera is needed and lawful. Due to the technology, all possible measures have been take to protect peoples data.

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, we are looking at unidentified idnviduals the coverage does not impact any particular groups. This is not a public site and an expextion of privacy is reduces as they are knowingly treaspassing.

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.	Nomad Multi Cam	Rapid Vision HD Multi camera	£12,000	3 full HD PTZ, i fixed Sentry HD defensive camera	Mobile camera unit deployed into Crime/ASB hot spot areas. camera is to cover set area were Crime/ASB is being reported.

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.	Pavillion Gable over looking pathway to changing room.	Nomad Multi Cam	£12, 000+inst all cost	24hr, 30 day day memory capcity	Post review	This deployment has a specific reason for deployment (responding to a New ASB hotspot) and has a clear operational need. (to reduce ASB at the Location) The deployment has a clarity of purpose (The camera will ben used to identify the offenders and enforce via the Incremental approach. There is a belief that this group is known from the work earlier this year at the Royal hotel. The camera will be able to confirm this.

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)
Camera				

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	
Camera location	

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	
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	
Date	

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

Name	Nicola Taylor
Date	10/12/2019
Summary of DPO advice	Processing can proceed Legitimate purpose for deploying the camera with evidence of ASB Lawful basis for processing under Article 6(e) GDPR and Schedule 2 Part 1 Paragraph 2 DPA 2018.

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

Name	
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

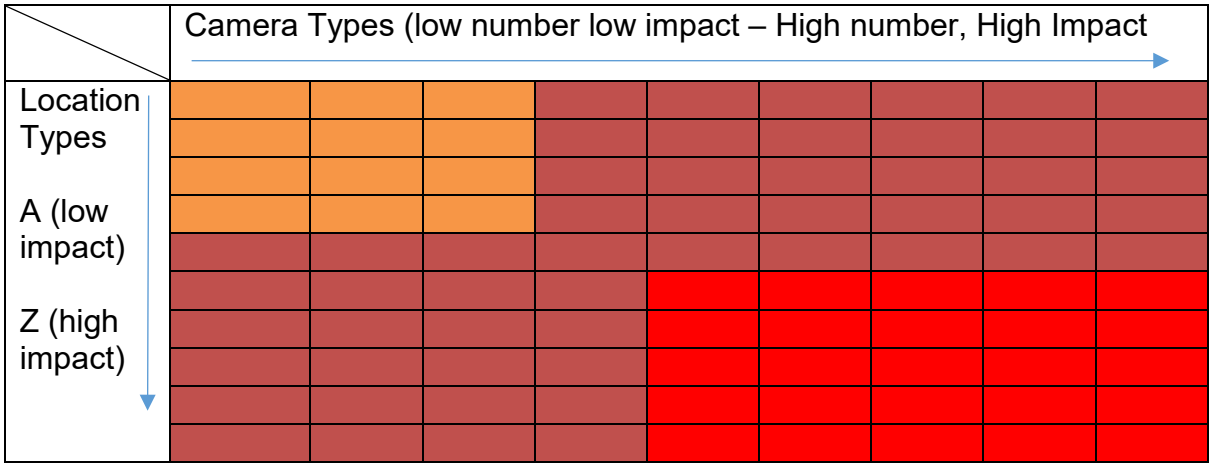
Name	
Date	

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:



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)

Mobile CCTV unit-Nomad Multi Camera

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.

Hard drive built in to the cameras accessed remotely from CCTV control room. All acess is fully auditable.

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 data is secure and encrypted. the equipment is desigened for this use and is current and up tode all OS updates.

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 or Short range wifi. preffered option is 4G access.

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

encrypted, 2 teir password. access terminal is in a secure location. it is only acrtive when in use. IE turned off when not in use. LAPTOP is updated.

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)

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?

System is secure by design and this was part of the process to purchase the camera. As far as we can assert, this is a Secure system using bespoke access via a secure laptop

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)

We are looking for suspect ASB and criminal damage. the safety of the young people is also a concern. in a specific location. information only shared with the Police.

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

30 days

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)

memory is wiped post deployment

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)

Full CCTV seziure process used

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)

Police evidence process and built in auditable function on the laptop.

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)

Permenant~~inante~~ Opera~~ter~~tors are SIA badged and Community Safety Team Leader. Staff are trained to use this system. ASll staff have been trained to SIA CCTV (public Space) Lv2.

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

Appendices- NWLDC Privacy statements

CCTV and Personal Information

Most usage of CCTV will be covered by the Data Protection Act 2018. This gives you the right to see information held about you, including CCTV images of you, or images which give away information about you (such as your car number plate).

The Data Protection Act sets rules which CCTV operators must follow when they gather, store and release CCTV images of individuals. The Information Commissioner can enforce these rules.

You can see the ICO's advice to operators in The Information Commissioner's CCTV Code of Practice.

Some uses of CCTV are not covered by the Data Protection Act. For example, the use of cameras for limited household purposes (such as to protect a home from a burglary) - even if the camera overlooks the street (for more information on this, see The Information Commissioner's FAQs).

If you are concerned that CCTV is being used for harassment, anti-social behaviour or other matters dealt with under criminal law, then these are matters for the police. Images taken for recreation, such as on mobile phones, digital cameras and camcorders, are also exempt from the Act.

Law enforcement covert surveillance activities are covered by a separate Act - the Regulation of Investigatory Powers Act (RIPA) 2000 and the Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000.

Data Protection Subject Access CCTV

Public CCTV is a successful part of the tools developed during recent years to assist with efforts to combat crime and disorder whilst enhancing community safety.

Equally, it may be regarded by some as the most potent infringement of people's liberty. If users, owners and managers of such systems, are to command the respect and support of the general public, the systems must not only be used with the utmost probity at all times, they must be used in a manner which stands up to scrutiny and is accountable to the very people they are aiming to protect.

We are committed to the belief that everyone has the right to respect for his or her private and family life.

Although the use of Public CCTV cameras has become widely accepted in the UK as an effective security tool, those people who do express concern tend to do so over the handling of the information (or data) which the system gathers.

After considerable research and consultation, this Council has adopted a nationally recommended standard.

Please read this page fully before applying for data. The forms to apply for data are at the bottom of this page

Please also note: CCTV images are kept secure for 31 days - after which they are destroyed unless the footage is required by the police in connection with a crime

Primary request to view data

Primary requests to view data generated by a CCTV system are likely to be made by third parties for any one or more of the following purposes:

Providing evidence in criminal proceedings (e.g. Police and Criminal Evidence Act 1984, Criminal Procedures & Investigations Act 1996, etc.)
Providing evidence in civil proceedings or tribunals
The prevention of crime
The investigation and detection of crime (may include identification of offenders)
Identification of witnesses
Third parties, which should be required to show adequate grounds for disclosure of data within the above criteria, may include, but are not limited to:

- Police
- Statutory authorities with powers to prosecute, (e.g. Customs and Excise, Trading Standards etc)
- Solicitors
- Claimants in civil proceedings
- Accused persons or defendants in criminal proceedings
- Other agencies, according to purpose and legal status, as agreed by the Data Controller and notified to the Information Commissioner
- Upon receipt from a third party of a bona fide request for the release of data, the scheme owner (or representative) should:

Not unduly obstruct a third party investigation to verify the existence of relevant data
Ensure the retention of data which may be relevant to a request, but which may be pending application for, or the issue of, a court order or subpoena, (it may be appropriate to impose a time limit on such retention which should be notified at the time of the request)
A time limit could apply providing reasonable notice was issued to the agent, prior to the destruction of the held data, (eg a time limit was about to expire).

Where requests fall outside the terms of disclosure and Subject Access legislation, the data controller, or nominated representatives, shall:

Be satisfied that there is no connection with any existing data held by the police in connection with the same investigation
Treat all such enquiries with strict confidentiality
A Data Controller can refuse an individual request to view if insufficient or inaccurate information is provided. A search request should specify reasonable accuracy (could be specified in ½ hour).

Secondary request to view data

A 'secondary' request for access to data may be defined as any request being made, which does not fall into the category of a primary request.

Before complying with a secondary request, the scheme owner should ensure that:

- The request does not contravene, and that compliance with the request would not breach, current relevant legislation, (e.g. Data Protection, section 163 Criminal Justice and Public Order Act 1994, etc.)

- Any legislative requirements have been complied with, (e.g. the requirements of the Data Protection Act)

- Due regard has been taken of any known case law (current or past) which may be relevant, (e.g. R v Brentwood BC ex p. Peck) and

- The request would pass a test of 'disclosure in the public interest'

If, in compliance with a secondary request to view data, a decision is taken to release material to a third party, the following safeguards should be put in place before surrendering the material:

In respect of material to be released under the auspices of 'crime prevention', written agreement to the release of the material should be obtained from a police officer, not below the rank of Inspector. The officer should have personal knowledge of the circumstances of the crime/s to be prevented and an understanding of the CCTV System Code of Practice
If the material is to be released under the auspices of 'public wellbeing, health or safety', written agreement to the release of material should be obtained from a senior officer within the Local Authority. The officer should have personal knowledge of the potential benefit to be derived from releasing the material and an understanding of the CCTV System Code of Practice
Recorded material may be used for bona fide training purposes such as police or staff training. Under no circumstances will recorded material be released for commercial sale of material for training or entertainment purposes.

Individual subject access under data protection legislation

Under the terms of Data Protection legislation, individual access to personal data, of which that individual is the data subject, must be permitted providing:

- The request is made in on the correct form giving correct information
- A fee is no longer required for each individual search
- The Data Controller is supplied with sufficient information to satisfy him or herself as to the identity of the person making the request

The person making the request provides sufficient and accurate information about the time, date and place to enable the data controller to locate the information, which that person seeks, (it is recognised that a person making a request is unlikely to know the precise time. Under those circumstances, it is suggested that within one hour of accuracy would be a reasonable requirement) under those circumstances, it is suggested that within one hour of accuracy would be a reasonable requirement)

The person making the request provides sufficient and accurate information relevant to the particular search and which contains personal data of him or herself only, unless all other individuals who may be identified from the same information have consented to the disclosure
In the event of the scheme owner complying with a request to supply a copy of the data to the subject, only data pertaining to the individual should be copied, (all other personal data which may facilitate the identification of any other person should be concealed or erased). Under these circumstances an additional fee may be payable.

The data controller is entitled to refuse an individual request to view data under these provisions if insufficient or inaccurate information is provided. However every effort should be made to comply with subject access procedures and each request should be treated on its own merit.

In addition to the principles contained within the Data Protection legislation, the data controller should be satisfied that the data is:

- Not currently and, as far as can be reasonably ascertained, not likely to become, part of a 'live' criminal investigation
- Not currently and, as far as can be reasonably ascertained, not likely to become, relevant to civil proceedings
- Not the subject of a complaint or dispute which has not been actioned
- The original data and that the audit trail has been maintained
- Not removed or copied without proper authority
- For individual disclosure only (i.e. to be disclosed to a named subject)

Process of disclosure

- Verify the accuracy of the request.

- Replay the data to the requester only, (or responsible person acting on behalf of the person making the request)

- The viewing should take place in a separate room and not in the control or monitoring area. Only data, which is specific to the search request, should be shown

- It must not be possible to identify any other individual from the information being shown; (any such information should be blanked-out, either by means of electronic screening or manual editing on the monitor screen).

- If a copy of the material is requested and there is no on-site means of editing out other personal data, then the material should be sent to an editing house for processing prior to being sent to the requester.

Media disclosure

In the event of a request from the media for access to recorded material, the procedures outlined under 'secondary request to view data' should be followed. If material is to be released the following procedures should be adopted:

- The release of the material must be accompanied by a signed release document that clearly states what the data will be used for and sets out the limits on its use
- The release form should state that the receiver must process the data in a manner prescribed by the data controller, e.g. specify identities/data that must not be revealed
- It may also require that proof of editing must be passed back to the data controller, either for approval or final consent, prior to its intended use by the media (protecting the position of the data controller who would be responsible for any infringement of Data Protection legislation and the System's Code of Practice)
- The release form should be considered a contract and signed by both parties