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:

Corsham, Wiltshire: This is a retrospective assessment based on historic installation of a mobile CCTV system used periodically at the following locations: Springfield Recreation Ground and surrounding area; High Street; Town Hall; Pickwick Road/Newlands Road junction; High Street Car Park, and Katherine Park. It also covers five fixed cameras in the Town Hall entrance and foyer.

Date of assessment	25/10/2019 (first in this format)
Review date	January 2026
Name of person responsible	David Martin, Chief Executive (CEX)
Name of Data Protection Officer	One West

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.

For the prevention and detection of crime and anti-social behaviour and protection of property at various locations in Corsham. The system also promotes community safety. Wiltshire Police provides the Town Council with monthly reports on crimes recorded in Corsham.

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.

The mobile CCTV system helps protect Town Council assets; increases personal safety and helps reduce the fear of crime; it supports the Police in a bid to deter and detect crime; and it assists the Police in identifying, apprehending and prosecuting offenders.

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.

The system only operates where there is adequate lighting. It is operational 24/7 as offences occur at all times of day and night, and the fear of crime is heightened at night. Each location covered by the CCTV camera is open and accesssible at all times, apart from the Town Hall which is locked and alarmed when not in use.

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: Legitimate Interests.

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**.

See Appendix Three.

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.

Community Safety is important to the Town Council for the health and wellbeing of residents and visitors. There is a general view that people who are not involved in crime are happy to be in an area covered by CCTV. Our system is only used for crime prevention and detection purposes, which are beneficial to the wider public.

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

The main benefits are: protection of property; an enhanced feeling of community safety; retrospective investigation of incidents and crime prevention. The CCTV system provides evidence for use in prosecutions.

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 is maintained by directing the CCTV camera away from private property and limiting the number of authorised people who can access the system. Images are automatically deleted after 31 days. The system is not used to covertly monitor staff or visitors. The images are only shared with those listed in Appendix Three. The impact on individuals is positive as it leads to a safer environment.

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 CCTV camera locations and areas they cover have been selected with privacy in mind. The cameras are kept in a static position with tilting/panning features turned off. Whilst privacy masking features can be useful, we avoid overlooking an area in the first place if it is likely to concern neighbours.

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 images will be used by Corsham Town Council and the Police for the investigation of crime and antisocial behaviour and evidential purposes only.
The Data Controller is Corsham Town Council.

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 images need to recognise individuals so that they can be identified to provide evidence for the investigation of crime and antisocial behaviour, including helping eliminate suspects from Police enquiries.

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.

Signage is in place in the vicinity of the CCTV cameras, explaining that the area they are entering is covered by CCTV.
Policies and procedures are in place for responding to Subject Access Requests and other requests for information. The Privacy Notice is available on the Town Council's website (www.corsham.gov.uk).

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 is reviewed periodically and reported to the Town Council's Property and Amenities Committee.
The Town Council's Risk Management processes deal with safety and security. Regular meetings are held with our ICT service provider and the DPA 2018/GDPR requirements are discussed at regular team meetings.

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?

There are no plans to extend the scope of the current mobile CCTV system. A new Data Protection Impact Assessment would be carried out prior to commissioning any changes. A second mobile CCTV camera was purchased in 2022. It is deployed in the same locations as the original camera.
There are four wireless and one wired CCTV cameras in the Town Hall foyer and entrance to help protect property and staff.

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 system has been set up on a proper and legal basis and is compliant with the Data Protection Act 2018, Human Rights Act and other legal requirements. The system is reviewed at least annually to justify the need.

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.

The CCTV system, policies, processes and locations selected do not discriminate against individuals or groups.

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.	Wireless Mobile Camera	WCCTV Wireless Dome	2no.	Pan, tilt and zoom function. Automatic pan and tilt function not routinely used. Long zoom lens. Colour images.	Public space recording 24 hrs. Can be located in specified locations where needed around Corsham agreed with Police.
2.	General Camera	Samsung Smart Home Camera: HD Outdoor	1no.	Fixed position, integrated card reader.	Located in entrance foyer for the security and safety of Town Council staff/public and property. Images can be viewed via the Chief Executive's PC using the microSD card and adaptor.
3.	Wireless Camera	Tapo Camera: C420	4no.	Fixed position, with hub.	Located in the Town Hall foyer and entrance for the security and safety of Town Council staff/public and property. Images viewed via the Chief Executive's iPhone (App and login required).
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					

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.	Springfield Rec	1	1	24 hrs when the camera is put in this location.	Weekly check of functionality, plus infrequent ad hoc checks.	The privacy level expectation in a recreation ground is very low. The location is well signed with appropriate signage for CCTV, its purpose and with contact details. The site was selected due to reported crime and anti-social behaviour.
B.	High Street	1	1	24 hrs when the camera is put in this location	Weekly check of functionality, plus infrequent ad hoc checks.	The privacy level expectation in a town high street is very low. The location is well signed with appropriate signage for CCTV, its purpose and with contact details. The site was selected due to reported crime and anti-social behaviour.
C.	Town Hall, High Street (external)	1	1	24 hrs when the camera is put in this location	Weekly check of functionality, plus infrequent ad hoc checks.	The privacy level expectation in a town high street is very low. The location is well signed with appropriate signage for CCTV, its purpose and with contact details. The site was selected due to reported crime and anti-social behaviour.
D.	Pickwick Road/ Newlands Road junction	1	1	24 hrs when the camera is put in this location	Weekly check of functionality, plus infrequent ad hoc checks.	The privacy level expectation in a town centre is very low. The location is well signed with appropriate signage for CCTV, its purpose and with contact details. The site was selected due to reported crime and anti-social behaviour.
E.	High Street Car Park	1	1	24 hrs when the camera is put in this location	Weekly check of functionality, plus infrequent ad hoc checks.	The privacy level expectation in a public car park is very low. The location is well signed

CAT	Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
						with appropriate signage for CCTV, its purpose and with contact details. The site was selected due to reported crime and anti-social behaviour.
F.	Katherine Park	1	1	None. Historic site. No longer used.	N/A	The site would be re-assessed prior to any further use.
G.	Town Hall entrance/ foyer	2	5	24 hrs	Weekly check of functionality, plus infrequent ad hoc checks	Privacy level on entering a public building is low. The location is signed with appropriate signage for CCTV, its purpose and with contact details. The site was selected to protect property and staff. Prior to the CCTV system being installed, there were incidents of theft and damage.
H.						
I.						
J.						
K.						
L.						

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)
62	14/01/ 2019	CCTV Camera 1	Mobile CCTV	
-	-	-	-	
275	14/01/ 2019	CCTV Camera 2	Fixed - Town Hall Entrance	
325	05/04/202 2	CCTV Camera 3	Mobile CCTV	
348	24/08/202 3	CCTV Camera 4	Fixed - Town Hall Foyer	
348	14/12/202 3	CCTV Camera 5	Fixed - Town Hall Foyer	

Asset number	Reviewed	Camera type	Location category	Further mitigation/ comments (optional)
-	01/04/2025	CCTV Camera 6	Fixed - Town Hall Entrance	
-	01/04/2025	CCRTV Camera 7	Fixed - Town Hall Entrance	

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	N/A
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	David Martin
Date	01/04/2025

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	One West
Date	19/12/2023
Summary of DPO advice	No further additions.

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

Name	
Date	
Comments	

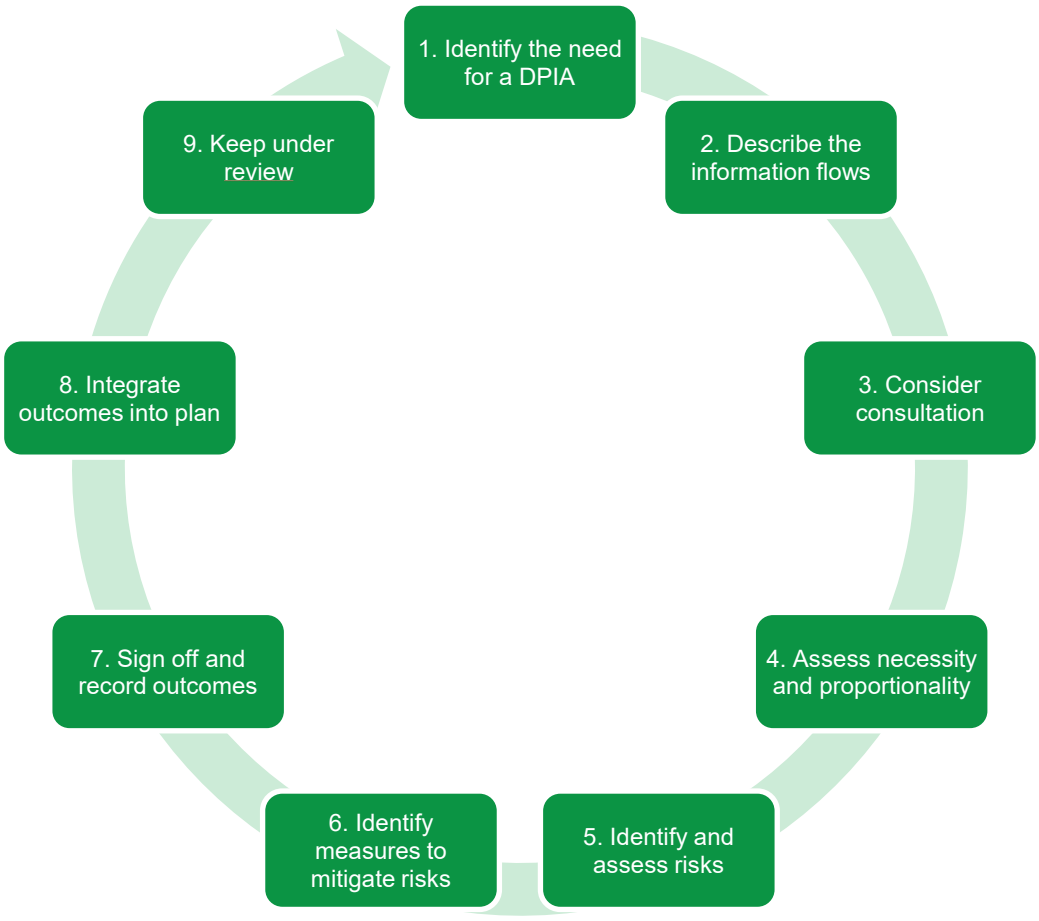
Consultation responses reviewed by:
If your decision departs from individuals' views, you must explain your reasons

Name	
Date	
Comments	

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

Name	Sean Smythe (DPO - One West) - refer to email
Date	14/01/2026

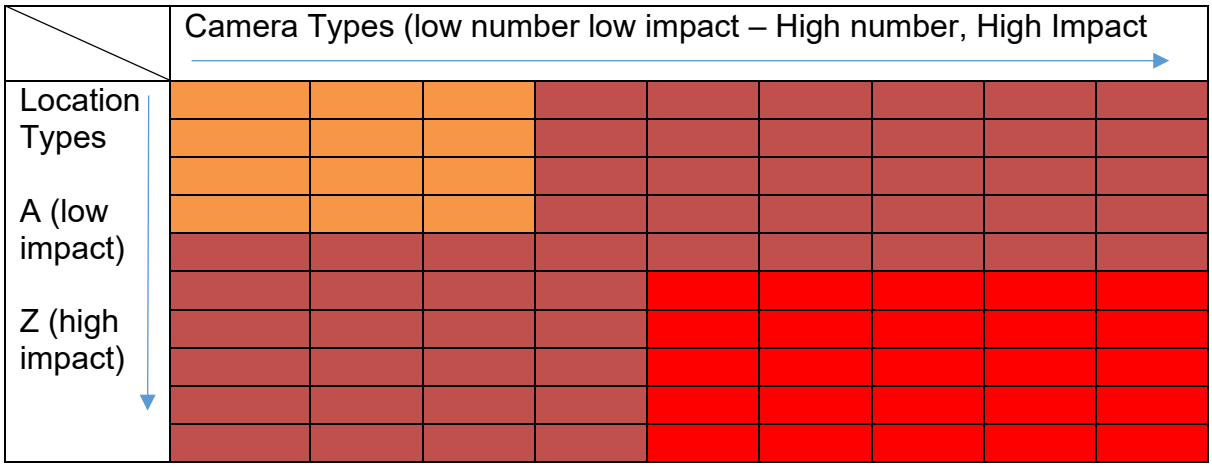
APPENDIX ONE: STEPS IN CARRYING OUT A DPIA



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)

Real time monitoring only takes places for a few minutes each week to ensure the systems are functioning correctly.

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.

WCCTV: On-site. The data can also be accessed remotely from the Town Hall via the CEX's PC and iPhone and by the Technical Assistant's Laptop and iPhone. There is no audio-recording.
Town Hall CCTV: On-site (SD card and cloud). The data can be accessed remotely via the CEX's iPhone. Audio-recording is switched off.

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. Access is restricted to authorised Town Council staff (Members of the Senior Management Team and Technical Assistant) and the Police. The images, including live feed, can only be seen via certain computers and kept securely in the Town Hall. A VPN and password are needed to access the CCTV software. The software is only used when needed and not left running at other times. It can also be viewed via the CEX's PC, laptop and/or iPhone.

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)

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

Ironshare Security, Windows Security, Threatdown Endpoint Agent and Email Security, and Cisco Secure Client. This is managed by Onecom.

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)

Springfield; High Street; Town Hall; Pickwick Road/Newlands Road junction; High Street Car Park, and Katherine Park; Town Hall (internal public area - entrance and foyer)

☐ 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?

ICT Contract with Onecom. This covers security of the Town Council ICT systems. Contract meetings flag up any issues and risks. We receive monthly cyber security reports. The Chief Executive completes an annual cybersecurity checklist.

5.8 How is the information used? (tick multiple options if necessary)

- ☐ Monitored in real time to detect and respond to unlawful activities
- ☐ Monitored in real time to track suspicious persons/activity
- ☐ Compared with reference data of persons of interest through Automatic Facial Recognition software
- ☐ Compared with reference data for vehicles of interest through Automatic Number Plate Recognition software
- ☐ Used to search for vulnerable persons
- ☐ Used to search for wanted persons
- ☒ Recorded data disclosed to authorised agencies to support post incident investigation by, including law enforcement agencies
- ☒ Recorded data disclosed to authorised agencies to provide intelligence
- ☐ Other (please specify)

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

31 days. Images may occasionally be stored for longer periods for evidential purposes.

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)

Upon request, the Police may request that certain images or footage is retained for evidential purposes.

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)

We would release images to where legally required to do so.
We may use images in support of an insurance claim made by ourselves.

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)

Disclosed in person in hard copy or, rarely, memory stick (password protected) or sent via secure email. Police can also take screenshots or photos of desktop images.

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)

The independent Data Protection Officer is permitted access to all policies and procedures for auditing purposes.

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)

The in-house training provides an overview of the system for those authorised to use it. Detailed information is available as part of the Town Council's general policies, procedures and staff handbook.

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