SURVEILLANCE CAMERA COMMISSIONER

ico.
Information Commissioner's Office

Data protection impact assessments template for carrying out a data protection impact assessment on surveillance camera systems

Project name: CCTV Upgrade - Camera Scheme Expansion - Camera 64 - Bidford-upon-Avon / Camera 39 and Camera 40 - Darlingscote Road, Shipston on Stour

Data controller(s): Stratford-on-Avon District Council

This DPIA template should be completed with reference to the guidance provided by the Surveillance Camera Commissioner and the ICO. It will help you to identify whether the use of surveillance cameras is appropriate for the problem you wish to address, assess the risks attached to your project and form a record of your decision making.

1. Identify why your deployment of surveillance cameras requires a DPIA[1]:

☐ Systematic & extensive profiling	☐ Large scale use of sensitive data
☒ Public monitoring	☐ Innovative technology
☐ Denial of service	☐ Biometrics
☐ Data matching	☐ Invisible processing
☐ Tracking	☐ Targeting children / vulnerable adults
☐ Risk of harm	☐ Special category / criminal offence data
☐ Automated decision-making	☐ Other (please specify)

Public space town centre monitoring for crime prevention and detection of crime and public safety

2. What are the timescales and status of your surveillance camera deployment?
Is this a proposal for a new deployment, or the expansion of an existing surveillance camera system? Which data protection regime will you be processing under (i.e. DPA 2018 or the GDPR)?

Expansion of existing CCTV surveillance camera system. 2 x P/T/Z CCTV and 1 x Static CCTV camera to be added to existing town centre system monitored, maintained and certified in accordance with the SCC code of practice and governing guidance. GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of offical authority vested in the controller.

Describe the processing

3. Where do you need to use a surveillance camera system and what are you trying to achieve?
Set out the **context** and **purposes** of the proposed surveillance cameras or the reasons for expanding an existing system. Provide evidence, where possible, including for example: crime statistics over an appropriate time period; housing and community issues, etc.

The location of the CCTV cameras are 1) The Big Meadow, Bidford-on-Avon and 2) Darlingscote Road and Shipston Leisure Centre, Shipston-on-Stour

The following objectives have been established for the Stratford-on-Avon District Council CCTV and associated systems:

[1] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

a) reducing fear of crime
b) deterring and preventing crime
c) assisting in the maintenance of public order and reducing offences involving vandalism and nuisance
d) providing high quality evidence which may assist in the detection of crime and the apprehension and prosecution of offenders
e) protecting property
f) providing assistance with civil claims
g) providing assistance with issues relating to public safety and health
h) providing assistance and reassurance to the public in emergency situations

Bidford-on-Avon:

Stratford-on-Avon District Council has an established CCTV scheme which is used to detect and prevent crime and provide public reassurance.

The area where this camera is to be installed is a busy recreational ground which is used by many of the residents of Bidford and attracts both visitors and event organisers from outside of the village. The CCTV camera would also cover the main arterial route directly in to the town, which is currently uncovered by CCTV. The area also includes a partial view of Bidford High Street and a view of a key car park for the Big Meadow. This CCTV camera will provide evidence and the ability to catch and apprehend offenders coming in and out of Bidford. There are a number of key hotspots for Anti-social Behaviour within the prosepctive CCTV scope, including the park itself. The presence of a CCTV camera will assist the evidence gathering of ASB taking place in the area. There are a number of key businesses/ buildiings in the area including the cricket/sports pavillion.

Historically there have been considerable public concerns about a range of offences in the park and residents reporting feeling unsafe. There is also considerable public concern relating to traffic offences relating to the Honeybourne road and the historic bridge that joins with Bidford High Street.

Criminal Offences within the CCTV Zone (Annex A)

In total there were 43 offences recorded within the 300m CCTV zone during the examined period. The reporting period for this was May 2018 to April 2019 (Warwickshire Insight Service). The recurring categories of offences were:

Other Theft (9)
Assault with injury (7)
Assault Without Injury (7)
Burglary - Business and community (4)
Public Fear, Alarm or Distress (4)
Theft From A Vehicle (3)
Criminal Damage To A Vehicle (2).

There were also 12 incidents of Anti-Social Behaviour during this period. There was also 1 Road Traffic Collisions that occurred.

More recent analysis from June 2020 to June 2021 shows that within 200 metres of the camera there were:

June 2021- 11 Incidents
May 2021- 6 Incidents
April 2021- 9 Incidents
March 2021- 5 Incidents
Febuary 2021- 1 Incident
January 2021- 4 Incidents
December 2020- 2 Incidents
November 2020- 1 Incident

October 2020- 4 Incidents
September 2020- 1 Incident
August 2020- 2 Incidents
July 2020- 4 Incidents
June 2020- 5 Incidents

Additional crime statistics can be found online

Shipston on Stour

Stratford-on-Avon District Council has an established CCTV scheme which is used to detect and prevent crime and provide public reassurance.

Stratford-on-Avon District Council has an established CCTV scheme which is used to detect and prevent crime and provide public reassurance. The area where this camera is to be installed is a main arterial route into Shipston, which is currently uncovered by CCTV. The area also has a high school, a leisure centre and a skate park within view which have all previously reported crime or anti-social behaviour. There are also a number of buisnesses in the area. The CCTV camera will provide evidence and an ability to apprehend offenders coming in and out of Shipston.

Significant concern has been raised by local residents, community representatives and councilors about ongoing ASB at the location.

Criminal Offences within the CCTV Zone (Annex A)

In total there were 21 offences recorded within the 300m CCTV zone during the examined period. The reporting period for this is May 2018 to April 2019 . (Warwickshire Insight Service) The recurring categories of offence were:
Assault with Injury (3)
Criminal Damage to vehicle (3)
Malicious Communication (3)

There were also 27 Incidents of Anti-Social Behaviour that occurred during this period.

More recent analysis from June 2020 to June 2021 shows that within 200 metres of the camera there were:

June 2021- 4 Incidents
May 2021- 2 Incidents
April 2021- 6 Incidents
March 2021- 1 Incidents
Febuary 2021- 2 Incidents
January 2021- 5 Incidents
December 2020- 3 Incidents
November 2020- 0 Incidents
October 2020- 2 Incidents
September 2020- 5 Incidents
August 2020- 3 Incidents
July 2020- 4 Incidents
June 2020- 4 Incidents

Additional crime statistics can be found online

4. Whose personal data will you be processing, and over what area? Set out the **nature** and **scope** of the personal data you will be processing. Who are the data subjects, and what kind of information will you be collecting about them? Do they include children or vulnerable groups, and what is the scale and duration of the processing?

To meet the purpose of the CCTV scheme, the data captured must be of a quality capable of identifying person(s) who may be commiting, be victims of, or witnesses to crime or anti social behaviour. CCTV data is frequently used in criminal court proceedings so must be consistantly maintained to be of peak evidential quality.

The type of data being collected will include, height, sex, IC status, distinguishing features, clothing, directions of travel, vehicle registration numbers and vehicle types & colours. The CCTV system cannot discriminate in any way, nor does it have any analytical software which could be used to discriminate people.

The CCTV camera will be in a town centre area which will be visited by members of the public, children and vulnerable persons / groups. Collection of data is specific to prevention and detection of crime, public safety and the other purposes of the scheme listed in Section 3 above. The data collected and processed is in the form of recorded video footage. There will be images of children, vunerable persons, people from minority ethnic groups and religious beliefs however this will not be known at the time of recording unless the cameras are being proactively used by trained operating staff.The processing of the data will be proportionate to the achieving of the purposes listed therein.

Any proactive monitoring of the public must be justified by the operator. A full audit trail is maintained and inspected by the system supervisor on a regular basis. Images of individuals will only be released to investigating authorities in accordance with the objectives listed in the code of practice. The system will be used in an overt manner and signage informing the public that cctv is in operation will be displayed on routes prior to entering the CCTV camera scope.

Data is recorded continuously. The retention periods is 30 days after which there is an automatic deletion of the footage, unless required for criminal investigation/prosecution.

5. Who will be making decisions about the uses of the system and which other parties are likely to be involved? Will you be the sole user of the data being processed or will you be sharing it with other organisations or agencies? Record any other parties you would disclose the data to, for what purposes, and any relevant data sharing agreements. Note that if you are processing for more than one purpose you may need to conduct separate DPIAs.

Access to images by third parties will only be allowed in limited and prescribed circumstances. Disclosure will be limited to the following:-

a) law enforcement agencies where the images recorded would assist in a specific criminal enquiry
b) prosecution agencies
c) legal representatives
d) The media, where it is assessed by the Police that the public's assistance is needed in order to

assist in the identification of victim, witness or perpetrator in relation to a criminal incident. As part of that assessment the wishes of the victim of an incident should be taken into account.
e) The people whose images have been recorded and retained (Data Subject) unless disclosure to an individual would prejudice the criminal enquiries or criminal proceedings.

6. How is information collected? (tick multiple options if necessary)

- ☒ Fixed CCTV (networked)
- ☐ Body Worn Video
- ☐ ANPR
- ☐ Unmanned aerial systems (drones)
- ☐ Stand-alone cameras
- ☐ Redeployable CCTV
- ☐ Other (please specify)

7. Set out the information flow, from initial capture to eventual destruction. You may want to insert or attach a diagram. Indicate whether it will include audio data; the form of transmission; the presence of live monitoring or use of watchlists; whether data will be recorded; whether any integrated surveillance technologies such as automatic facial recognition are used; if there is auto deletion after the retention period. You may have additional points to add that affect the assessment.

Data will be captured in video format. The system is a combination of predominantly BT fibre and some additional wireless technology which is protected by a maintained firewall.There is live monitoring by SIA Front Line CCTV Licensed and vetted CCTV operators from the sole CCTV control room.

There is no automated facial recognition technology or audio recording. Staff will be provided with intelligence by the police relating to crime hotspots, wanted and missing persons under data sharing protocol.

The retention periods is 30 days after which there is an automatic deletion of the footage unless required for criminal investigation/prosecution.. Procedures, data sharing and security are in line with Stratford-on-Avon District Council policy and procedures.

Authorised staff have received relevant training in legislation, procedures and use of the system. Footage may be retained in an evidence locker for more than 30 days where a reasonable and necessary amount of data has been retained for investigation, subject access request or civil claim. Unless exceptional or unique circumstances apply, this data will be manually deleted after 12 calendar months. The evidence locker is reviewed by the supervisor and/or designated CCTV operator on a monthly basis. The principles of GDPR/DPA 2018 will be applied at all times.

8. Does the system's technology enable recording?

☒ Yes ☐ No

If recording is enabled, state where it is undertaken (no need to stipulate address, just Local Authority CCTV Control room or on-site will suffice for stand-alone camera or BWV), and whether it also enables audio recording.

Local Authority CCTV Server room contained within secure CCTV Control room

9. If data is being disclosed, how will this be done?

☒ Only by on-site visiting

☒ Copies of footage released (detail method below, e.g. encrypted digital media, via courier, etc)

☐ Off-site from remote server

☐ Other (please specify)

Data disclosed for purposes of insurance/legal claims and other rare occasions following application, approval and checking can be sent via combined means of encrypted digital storage device and courier. Access passwords will be sent seperately via email upon receipt.

Police will access disclosed data within CCTV Control Room.

10. 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 processing of biometric data, such as facial recognition.

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

☐ Linked to sensor technology

☒ Used to search for vulnerable persons

☒ Used to search for wanted persons

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

☒ Recorded data disclosed to authorised agencies to provide intelligence

☒ Other (please specify)

Released to Licensing, Anti-social Behaviour and Environmental Health departments within the council for investigatory purposes

Consultation

11. Record the stakeholders and data subjects you have consulted about the deployment, together with the outcomes of your engagement.

Stakeholder consulted	Consultation method	Views raised	Measures taken
Local residents and businesses (Shipston-on-Stour)	Posted consultation	A Consultation questionnaire was sent to all residences and businesses within sight of the proposed CCTV Camera in December 19 / January 2020. 53 questionnaires were received back from residents and businesses which showed a majority of positive responses (98% support). 87% of respondents stated they agree or strongly agree clearly visible CCTV does not infringe on privacy.	Reinforced need for CCTV
Local residents and businesses (Bidford-on-Avon)	Posted consultation	A Consultation questionnaire was sent to all residences and businesses within site of the proposed CCTV Camera in December 19 / January 2020. 124 questionnaires were received back from residents and businesses which showed a majority of positive responses (87% support). 82% of respondents stated they agree or strongly agree clearly visible CCTV does not infringe on privacy.	Reinforced need for CCTV
CCTV Forum group	face to face consultation	Bidford-on-Avon and Shipston-on-Stour Town Council	Reinforced need for CCTV

Warwickshire Police	email / site visit	Highlighted problem areas and suggested best position for CCTV	Locations clarified
Stratford-on-Avon District Council's budget consultation 2019l	district wide consultationl	highlight residents would like to see an increase in the CCTV and Crime Reduction provision. Similar consultation work was undertaken in the last few years that showed a public desire to expand CCTV services (found online). Stratfords Citizens Panel also found that CCTV and Community Safety was the biggest area they wanted to see investment in (40% increase)	n/a
		.	

Consider necessity and proportionality

12. What is your lawful basis for using the surveillance camera system? Explain the rationale for your chosen lawful basis under the relevant data protection legislation. Consider whether you will be processing special categories of data.

The Data Protection Act 2018, Part 3: allows Stratford-on-Avon District Council as a competent authority to process personal data (including special category data) for the purposes of 1) detecting and preventing crime and 2) investigating and prosecuting criminal offences.

GDPR Article 6(1)(e): Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of offical authority vested in the controller.

Safer Warwickshire Partnership Board's information sharing protocol: The purpose of this protocol is to facilitate the lawful exchange of information, other than anonymised information, in order to comply with the statutory duty placed on the responsible authorities including Stratford-on-Avon District Council (Local Authorities, Police, Fire and Rescue, Health and Probation) to work together to develop and implement a strategy and tactics for reducing crime and disorder, anti social behaviour and substance misuse. This includes when an individual poses a risk of harm to the community, specific potential victims or professionals and any other behaviour affecting the local environment.

13. How will you inform people that they are under surveillance and ensure that they are provided with relevant information? State what privacy notices will be made available and your approach to making more detailed information available. Consider whether data subjects would reasonably expect to be under surveillance in this context.

Appropriate signage in and around the area where surveillance is taking place. QR code to be included on signage giving direction to Stratford-on-Avon District Council CCTV website

Consultation prior to installation as detailed above

Stratford-on-Avon District Council website provides information on location of cameras, statistics, privacy notice. SCC Self Assessment Tool, Code of Practice and DPIA.

14. How will you ensure that the surveillance is limited to its lawful purposes and the minimum data that is necessary for those purposes? Explain the adequacy and relevance of the data you will be processing and how it is limited to the purposes for which the surveillance camera system will be deployed. How will you know if it is delivering the benefits it has been deployed for?

Stratford-on-Avon District Council has installed CCTV cameras in various town centre, community hub and car park locations for the purposes of the prevention and detection of crime, disorder and anti-social behaviour. It is employed to reduce the fear of crime by helping to provide a safer environment for those people who live and work in the area and for visitors travelling to the area.

Prior to entering an area viewed by a CCTV camera, signs are displayed notifying you that CCTV is in operation, the purpose of the CCTV and also provides details of whom to contact for further information about the scheme. A QR code will be present on all new signs and those replaced in the future linking to the Stratford-on-Avon District Council CCTV website.
The purpose and use of the CCTV system are to provide the statutory prosecuting authorities and enforcement agencies with data to detect, deter and prevent crime. The images recorded must be maintained to a standard where it is possible to be used in the identification, apprehension and prosecution of offenders. The CCTV system installed by Stratford-on-Avon District Council must be able to provide the police and/or the district council with evidence to enable criminal and/or civil proceedings
Some examples of how we use your data are provided below;

• Providing evidence in criminal proceedings (police and criminal evidence act 1984 and criminal procedure and investigation act 1996)
• Providing evidence in civil proceedings
• The prevention and reduction of crime and disorder
• The investigation and detection of crime
• Identification of witnesses

Effectiveness of the system is measured in periodic performance indicators along with information supplied by the police and other council departments. Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012 and SC Code of Practice, GDPR/DPA is measured through the attainment Surveillance Camera Commissioner's Certification and British Standard 7958 accreditation.

An annual audit will be undertaken for the camera system, ensuring that each camera can reasonably be considered to capture data which supports the identified purposes above, captures new information not already captured by other cameras and also captures the minimum data possible to achieve these aims.

15. How long is data stored? (please state and explain the retention period)

Data is stored for a maximum of 30 days before it is automatically deleted by the digital management system. Data considered as evidential in value may be manually saved on an "evidence locker" for a period no more than 12 calendar months from the time and date of incident. 30 days is considered to sufficient for subject access requests and investigatory requests to be made. The evidence locker is regularly reviewed.

16. Retention Procedure

☒ Data 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)

Footage may be retained in an evidence locker for more than 30 days where required for an investigation, civil claim or subject access request. The evidence locker is reviewed on a monthly basis.

17. How will you ensure the security and integrity of the data? How is the data processed in a manner that ensures appropriate security, protection against unauthorised or unlawful processing and against accidental loss, destruction or damage? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Access is limited to the secure CCTV control room and system. The system incorporates passwords for authorised operators and is the subject of regular audits. The network has been upgraded, a firewall is in place and the system is security tested regularly.
DVD's are released to police officers, encrypted USB are released to third parties such as Insurance companies and solicitors via recorded delivery and email confirmation prior to disclosure of the encryption code. No international transfers are made.

18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information? Explain how you will provide for relevant data subject rights conferred under the legislation. 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.

Stratford-on-Avon District Council CCTV policies and procedures are fully compliant with the GDPR/DPA 2018 for general disclosure access requests and CCTV related subject access requests.

Information on subject access can be found on the Stratford-on-Avon District Council website and all requests are usually initially dealt with by the Information Governance Team and then passed to the CCTV Supervisor. On occasion a request is made directly to the CCTV Department/Commuity Safety Department which is then forwarded to the Information Governance Team.

https://www.stratford.gov.uk/online-forms/request-for-personal-data-or-other-information.cfm

Any complaints are dealt with through the councils complaints procedures.

https://www.stratford.gov.uk/council-democracy/how-to-complain.cfm

19. What other less intrusive solutions have been considered? You 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 continuous? Where you have considered alternative approaches, provide your reasons for not relying on them and opting to use surveillance cameras as specified.

Street lighting is already in abundance in both areas.

Continuous camera operation and recording is necessary as public space and offences can be at varied times.

Warwickshire Police conduct extra patrols in both areas and both area have been subject of discussion within partnership problem solving meetings with further actions currently being moved forward

Every deployment of CCTV is accompanied by a DPIA and public and stakeholder consulatation.

Privacy zones, which is standard software within modern CCTV cameras can be programmed. Alongside operator training, privacy notices and regular audits, this can help to mitigate any intrusion.

20. Is there a written policy specifying the following? (tick multiple boxes if applicable)

☒ The agencies that are granted access

☒ How information is disclosed

☒ How information is handled

Are these procedures made public? ☒ Yes ☐ No

Are there auditing mechanisms? ☒ Yes ☐ No

If so, please specify what is audited and how often (e.g. disclosure, production, accessed, handled, received, stored information)

All operation CCTV is subject to annual audit. This includes the use of cameras and downloading images, access, storage and incidents recorded. Regular audits are carried out by the CCTV Supervisor.

SSAIB conduct annual audit in compliance with British Standard 7958 and the Surveillance Camera Commisioner's Certification. The council also carries out it's own periodic audit.

Identify the risks

Identify and evaluate the inherent risks to the rights and freedoms of individuals relating to this surveillance camera system. Consider, for example, 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? Could it interfere with other human rights and freedoms such as those of conscience and religion, expression or association. Is there a risk of function creep? Assess both the likelihood and the severity of any impact on individuals.

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Non Compliance of GDPR/DPA 2018. The GDPR/DPA sets out seven key principles which Local Authority CCTV System owners must comply with whilst operating a Public Space Surveillance System: • Lawfulness, fairness and transparency • Purpose limitation • Data minimisation • Accuracy • Storage limitation • Integrity and confidentiality (security) • Accountability Non compliance may result in prosecution,financial penalties and severe damage to the reputation of Stratford-on-Avon District Council	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Compliance with articles 6, 8 and 14 of the Human Rights Act. The Act applies to public authorities and other bodies, which may be public or private, when they are carrying out public functions Article 6: the right to a fair trial Article 8: right to a private and family life	Possible	Significant	Medium

Article 14: protection from discrimination A breach of any article may impede on the subjects rights and result in the prosection of the local authority resulting in financial penalties and severe damage to its reputation			
Compliance with SC Code of Practice and the Protection of Freedoms Act 2012. The code of practice is issued by the Secretary of State under Section 30 of the 2012 Protection of Freedoms Act. Relevant authorities (as defined by section 33 of the 2012 Act) in England and Wales must have regard to the code when exercising any functions to which the code relates. A failure on the part of any person to act in accordance with any provision of the surveillance camera code does not of itself make that person liable to criminal or civil proceedings. The surveillance camera code is admissible in evidence in any such proceedings. (A court or tribunal may, in particular, take into account a failure by a relevant authority to have regard to the surveillance camera code in determining a question in any such proceedings. This is reflected in the Crown Prosecution Service Disclosure Manual) Reputational damage to Local Authority. The court may take inference in an authority's non compliance.	Possible	Significant	Medium
Security of Data. A Security Data breach may result in prosecution under GDPR/DPA 2018 and result in financial penalites and severe damage to the reputation of the local authority	Possible	Significant	Medium
Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**

Unauthorised Disclosure Unauthorised Disclosure may result in prosecution under GDPR/DPA 2018 and subject to financial penalites and severe damage to the reputation of the local authority	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Misuse of Data Misuse of data may result in prosecution under GDPR/DPA 2018 and subject to financial penalites and severe damage to the reputation of the local authority	Possible	Significant	Medium

Address the risks

Explain how the effects of privacy enhancing techniques and other features mitigate the risks you have identified. For example, have you considered earlier deletion of data or data minimisation processes, 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? What security features, safeguards and training will be in place to reduce any risks to data subjects. Make an assessment of residual levels of risk.

Note that APPENDIX ONE allows you to record mitigations and safeguards particular to specific camera locations and functionality.

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk			
Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Compliance with GDPR/DPA 2018. Management of the use and security of the system including monitoring and downloading of footage. Regular audits carried out and SCC Certification achieved.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Compliance with articles 4, 6 and 13 of the Human Rights Act Management of the use and security of the system including monitoring and downloading of footage. Regular audits carried out including proactive monitoring carried out by operators. SCC Certification achieved.	Reduced	Low	Yes
Compliance with SC Code of Practice and the Protection of Freedoms Act Management of system. SCC Full certification.	Reduced	Low	Yes

Options to reduce or eliminate risk	**Effect on risk**	**Residual risk**	**Measure approved?**
Security of Data Management of the use and security of the system including monitoring and downloading of footage. Regular audits carried out and SCC Certification achieved. Checks on proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Unauthorised Disclosure Release of data is strictly controlled by the council. Information Sharing Agreement in place with Police. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.	Reduced	Low	Yes
Misuse of Data Release and use of data is strictly controlled by the council. All parties who use data from the system are aware of their obligations under GDPR/DPA. Full audit trail for any release of data. CCTV staff trained in unauthorised disclosure and misuse of data.	Reduced	Low	Yes
Financial Loss. Compliance with GDPR/DPA, POFA, Code of Practice and operating procedures reduces the risk of unauthorised disclosure or the misuse of data. SCC Full certification achieved and regular audits are carried out by the system manager	Reduced	Low	Yes

Authorisation

If you have not been able to mitigate the risk then you will need to submit the DPIA to the ICO for prior consultation. Further information is on the ICO website.

Item	Name/date	Notes
Measures approved by:	Gerard Gray, IG Manager/DPO, 10/3/22 Phil Grafton,11/3/22	Integrate actions back into project plan, with date and responsibility for completion.
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.
DPO advice provided by:	Gerard Gray, Information Governance Manager	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice N/A		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by: Stuart Danskin		If your decision departs from individuals' views, you must explain your reasons.

Comments:		
This DPIA will be kept under review by: Stuart Danskin		The DPO should also review ongoing compliance with DPIA.

Date and version control: 19 May 2020 v.4

APPENDIX ONE

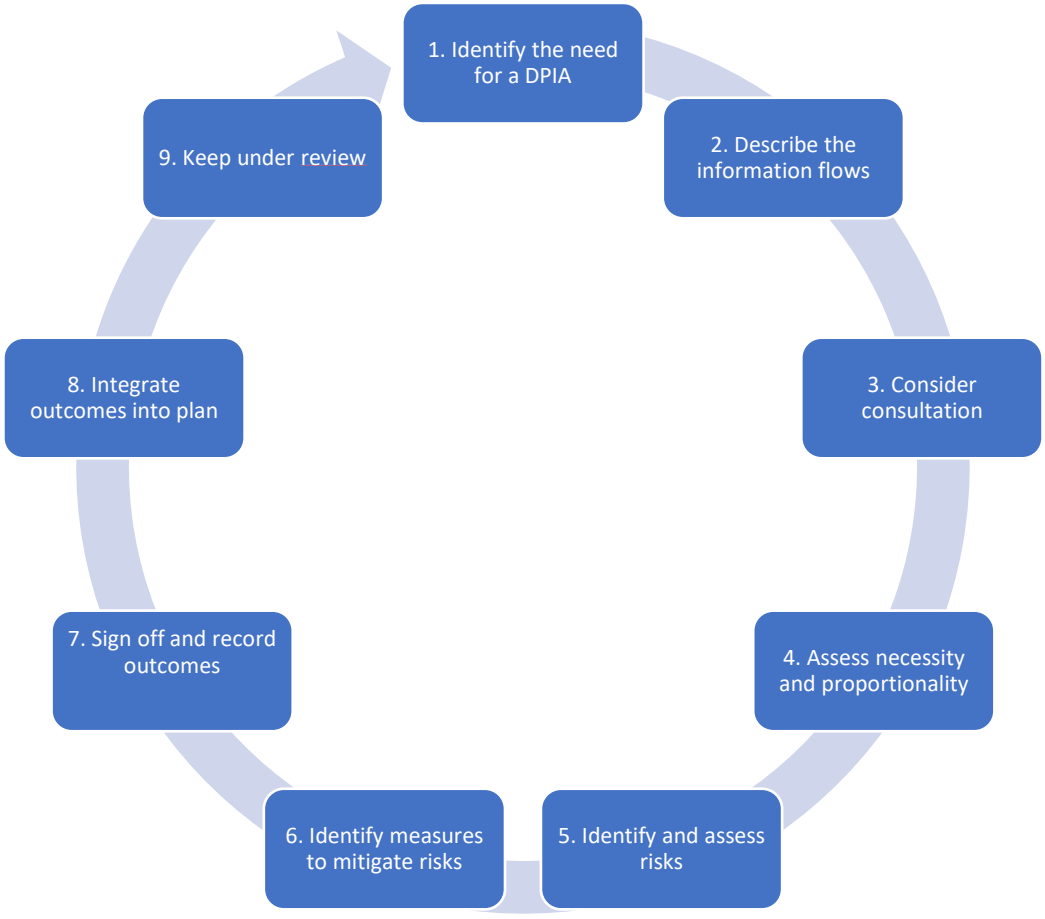
This template will help you to record the location and scope of your surveillance camera system and the steps you've taken to mitigate risks particular to each location.

Location: Each system operator/owner should list and categorise the different areas covered by surveillance on their system. Examples are provided below.

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
Public recreational area and thoroughfare Including underpass under busy arterial road	P/T/Z	2	24hours	24 hours (up to 2 CCTV operators)	The privacy level expectation in a public recreational area within town centre is very low; Historical problems of antisocial behaviour. Signage in place. Privacy blocking evaluated to be not necesary
Public Leisure Centre and associated facilities	Static	1	24hours	24 hours (up to 2 CCTV operators)	The privacy level expectation in a public recreational area within town centre is very low; Historical problems of antisocial behaviour. Signage in place. Privacy blocking evaluated to be not necesary

Date and version control: 19 May 2020 v.4

APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

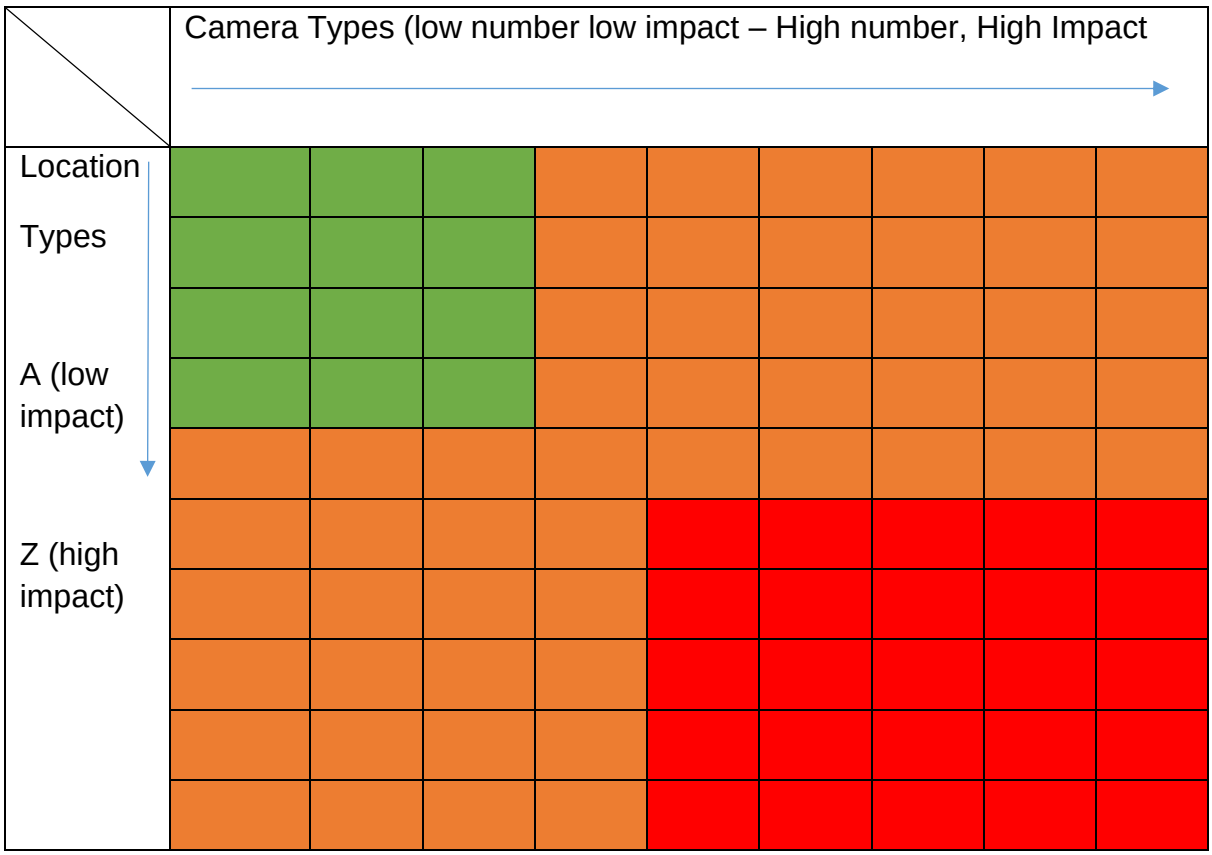


Date and version control: 19 May 2020 v.4

APPENDIX THREE: DATA PROTECTION RISK ASSESSMENT MATRIX

Use this risk matrix to determine your score. This will highlight the risk factors associated with each site or functionality.

Matrix Example:



Date and version control: 19 May 2020 v.4

NOTES

Date and version control: 19 May 2020 v.4

Date and version control: 19 May 2020 v.4