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: BCKLWN Public Space Surveillance CCTV System

Data controller(s): BCKLWN

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)

Assist the detection and prevention of crime in public spaces . Assist the council in its enforcement, traffic management, regulatory functions and safety of employees. Assist with public safety at many of the major events the council is involved in during the year.

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. Data Protection Act (DPA) 2018 or the General Data Protection Regulation (GDPR))?

The systems are existing CCTV systems which are monitored, maintained and certified in accordance with the Surveillance Camera Comissioner (SCC) Code of Practice,Security Industry Association (SIA), Approved Contractor Status (ACS), British Standard(BS)7858 and governing guidance. GDPR 6(1)e. Processing is necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller.

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.

CCTV cameras have been installed in town centres, public buildings, and other places to assist in the prevention and detection of crime, traffic management, to improve public safety and reduce anti-social behaviour. Bodyworn Video cameras are used by enforcement officers to assist the council with its regulatory functions and the safety of employees.

[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/

Monthly performance indicators of types of incidents,reviews and copies of footage requested are collected and published on the website. These can be found at https://www.west-norfolk.gov.uk/info/20154/cctv/513/cctv_statistics

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?

The council will process personal data of persons in public spaces and buildings, town centres, resorts and leisure facilities. The data collected is in the form of recorded video footage. There will be images of children and vunerable persons however this will not be known at the time of recording unless the cameras are being used proactively by staff .

Any proactive monitoring of the public must be justified by the operator.

A full audit trial is maintained and monotored by the system manager on a regular basis.Images of individuals wil 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 thorughout the locations.

The CCTV system does not discriminate in any way.

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.

The data ownder and data controller is BCKLWN. The council will share data under data sharing agreements with
1.Data subjects
2.Statutory prosecuting authorities
3.Clients and authorised investigators

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

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

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.

There is live monitoring by operators from the main CCTV control room or mobile vehicles if on site at an event.

All data is available to SIA licenced and BS7858/NPVV2 vetted operators in live and recorded video format.

The CCTV system is hardwired and transmitted using a combination of wireless technology, fibre, broadband and internal networked technology , most sites have an NVR recording on site that's accessed thorough the Councils secure ICT network back in the control room.

Some cameras also have audio equipment attached which can be activated during live incidents if necessary.

All recordings are auto deleted after the retention period of 28 days or less if the nvr is reaching capacity.

Footage is downloaded into a secure folder then deleted after 28 days.

If it is needed for further investigation it is then moved to a different secure folder with access limited to management only and is deleted as soon as possible. All data is kept within a secure network within the parameters of the Councils ICT extensive security requirements.All data viewed and/or released to third parties is recorded on a separate database.

All staff are have recived relevant training in legislation, procedures and use of the system and are vetted, licenced and continually trained in line with legislation and SIA requirements. Procedures,data sharing and security are in line with council policy and procdeures and the priciples of GDPR/DPA will be adhered to at all times.

Bodyworn footage is kept for 90 days to allow additional time for processing public requests/complaints. ANPR & standalone cameras used for enforcement and safety of employees are covered under separate procedures according to the needs of the service area and managed locally by them.

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.

CCTV Comms Room or On site.Some cameras allow audio is required for safety reasons but it is not automatically turned on. Bodyworn does allow audio recording.

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)

Footage can be accessed directly by the police or authorised authority or will be downloaded by request for the police or other authorities if necessary. Subject access requests, requests from insurance companies and solicitors can be requested by completion of a form on the website https://www.west-norfolk.gov.uk/info/20154/cctv/239/access_to_cctv and if released will be sent by recorded delivery.
All parties are required to sign a disclosure form for any media released.

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 council departments, trafiic management, partner authorites ,investigating ASB, Licensing and FlyTipping

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
Norfolk Constabulary	Email,phone, meetings	Requests to cover high crime, asb areas	Work with police and other agencies to assess sites , identify needs, funding, effectiveness and feasibility
BCKLWN service departments ie Noise & Nuisance	Emails,phone,meetings	Requests to cover problem areas	Work with relevant department/s and other agencies to assess sites , identify needs, funding, effectiveness and feasibility
Anti-Social Behaviour, Operational Partnership Team	Emails,phone,meetings	Snap meetings held consultation with public and views fed back	Work with ASB/OPT teams to assess needs and identfy solutions
Clients & Partner Authoritys	Emails,phone,meetings	Requests to cover facilities, areas of high crime and problem areas	Work with clients and partner authoritys to assess sites, identify and implement solutions
General Borough Council service areas	Emails,phone,meetings	Management of building services & facilities including investigation of accidents & incidents including access control	Work with relevant department/s and other agencies to assess sites , identify needs, funding, effectiveness and feasibility

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.

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.

Local authorities establish their CCTV systems under the GDPR/DPA and Section 17 Crime and Disorder Act 1998 which places an obligation on local authorities and the police to work in partnership to develop and implement a strategy for tackling crime and disorder and monitoring public events for Health &Safety purposes.

Section 17 outlines how and why local services may impact on crime and disorder and indicates the reasonable actions that might be put in place to ensure a co-ordinated approach to crime reduction. Evidence shows the opportunity for crime and disorder may be reduced and the safety and reassurance of the public improved when there is adequate CCTV coverage and it is used with other interventions.

Using CCTV remains a strategic, financial and operational choice in exercising crime reduction partnership responsibilities between the police and other relevant supporters.

In addition, Section 163 of the Criminal Justice and Public Order Act 1994 creates the power for local authorities to provide closed circuit television coverage of any land within their area for the purposes of crime prevention or victim welfare.

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.

Appropiate signage in and around the area where the cameras are placed.

Council website provides information on location of cameras, statistics, Surveillance Camera Commisioner Self Assessment Tool, Code of Practice and DPIA
https://www.west-norfolk.gov.uk/info/20154/cctv

Date: 01/04/23

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?

BCKLWN has installed CCTV (Closed Circuit Television) cameras in various locations for the purposes of reducing crime, disorder, anti-social behaviour and 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 through the area.. In all locations, signs are displayed notifying that CCTV is in operation and providing details of who to contact for further information about the scheme. The purpose and use of the CCTV system are to provide the Police and enforcement agencies with assistance to detect, deter and prevent crime and disorder; to help identify, apprehend and prosecute offenders; to provide the Police/Council with evidence to enable criminal and/or civil proceedings to be brought in the courts; and to maintain public order and safety of public and staff.

Effectiveness of the system is measured in monthly performamce indicators. Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012 and SC Code of Practice, GDPR/DPA is measured through SCC Certification process.

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

Footage is retained for 28 days depending on the location/nvr size when it is automatically deleted and overwritten. Bodyworn for 90 days.

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 is retained in the secure download folder for 28 days to ensure that the copy taken is not corrupted on the disc. It is then deleted unless it needs to be retained longer for major investigations, Civil Proceedings and Subject Access Requests. This retained footage is then reviewed regularly by management and deleted when it is considered to be no longer needed.

Date: 01/04/23

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 to the control room and system is restricted and fully auditable. The system has multi-layer authorisation levels and is subject to internal and external audits.
The council network is security tested regularly.
DVD's are released on non-writable discs while some other stakeholders supply their own secure copying media.

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.

The councils 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 BCKLWN council website and all requests are initially dealt with by the relevant manager.
https://www.west-norfolk.gov.uk/info/20154/cctv/239/access_to_cctv
Any complaints are dealt with through the councils coomplaints procedures.
https://www.west-norfolk.gov.uk/info/20190/have_your_say/426/comments_compliments_and_complaints

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.

Other solutions are always considered including the use of additional council resources such as ASB officers, lighting changes before CCTV is used. Every deployment of CCTV is accompanied by a DPIA, Privacy zones can be programmed to cameras along with operator training and regular audits can help to mitigate any potential intrusion.

Date: 01/04/23

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)

Any operations to do with CCTV are checked and audited both internally and externally. Annual audits are carried out by Security Systems Alarms & Inspection Board (SSAIB) to ensure compliance with SIA (Security Industry Authority) ACS (Approved Contractor Status), BS7958 CCTV Management and Operation, SCC (Surveillance Camera Commisioner) Code of Practice.

Date: 01/04/23

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 LA 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 the local authority	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	Possible	Significant	Medium

Article 8: right to a private and family life Article 14: protection from discrimination A breach of any article may impede on the subjects rights and result in the prosecution 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 authorites 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

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	Possible	Significant	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, reviewing 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, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved. Spot checks on proactive monitoring by staff	Reduced	Low	Yes
Compliance with SC Code of Practice and the Protection of Freedoms Act Management of system. SCC Full certification	Reduced	Low	Yes
Security of Data Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out and SCC Certification achieved. Spot checks on proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.	Reduced	Low	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:		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:		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA.

Date: 01/04/23

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)
Town Centre and local high street shopping areas	Static,PTZ, Body Worn	168	24hrs	24hrs	The privacy level expectation in a town centre is very low; our town centres are well signed with appropriate signage for CCTV its use and purpose with contact details.All recording and evidence downloads are secure and managed.
Public car park	Static,PTZ, Body Worn	134	24hrs	24hrs	The privacy level expectation in car parks is medium; all are well signed with appropriate signage for CCTV its use and purpose with contact details.All recording and evidence downloads are secure and managed.
Retail,Leisure Facilities, Industrial Estates and Resorts	Static, PTZ, Body Worn	292	24hrs	24hrs	The privacy level expectation in these facilities is very low; all areas are well signed with appropriate signage for CCTV its use and purpose with contact details.All recording and evidence downloads are secure and managed
Housing Estates & Residential Streets	Static,PTZ, Body Worn	49	24hrs	24hrs	The privacy level expectation in these areas is medium; all areas are well signed with appropriate signage for CCTV its

Date: 01/04/23

Location type	Camera types used	Amount	Recording	Monitoring	Assessment of use of equipment (mitigations or justifications)
					use and purpose with contact details.All recording and evidence downloads are secure and managed
Sites and Depots	Static, PTZ	164	24hrs	24hrs reactive	The privacy level expectation in these facilities is very low; all areas are well signed with appropriate signage for CCTV its use and purpose with contact details.All recording and evidence downloads are secure and managed
Parks,Play Areas	Static,PTZ	29	24hrs	24hrs	The privacy level expectation in these facilities is very low; all areas are well signed with appropriate signage for CCTV its use and purpose with contact details.All recording and evidence downloads are secure and managed
NHS, Health Education sector sites	Static, PTZ	87	24hrs	24hrs	The privacy level expectation in these facilities is high; all areas are well signed with appropriate signage for CCTV its use and purpose with contact details.All recording and evidence downloads are secure and managed
Body Worn Video	Separate units used whilst on shift	82	Whilst On shift	Whilst on shift	The privacy level expectation in using BWV is very low; the units are marked to say they are recording and the user will state this. All recording and evidence downloads are secure and managed.

Date: 01/04/23

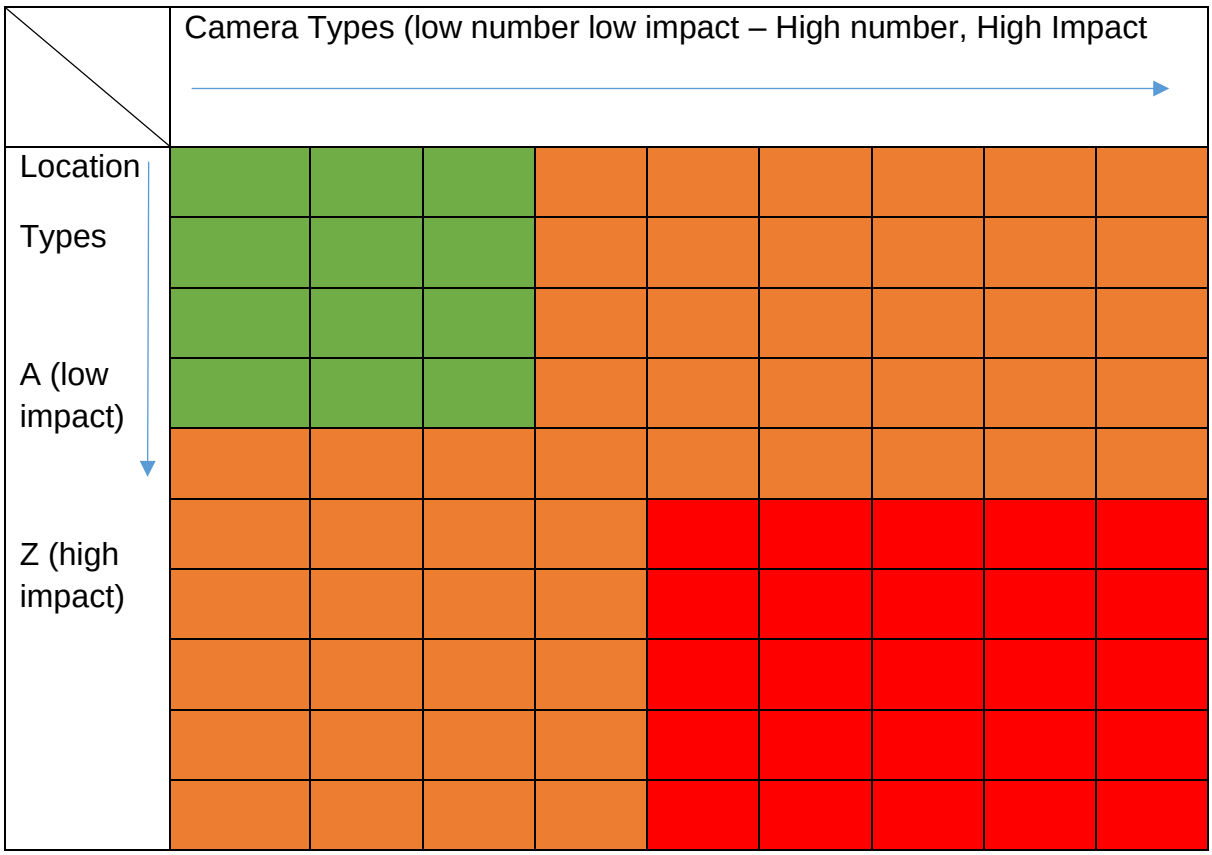
APPENDIX TWO: STEPS IN CARRYING OUT A DPIA

Date: 01/04/23

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: 01/04/23

NOTES

Date: 01/04/23

Date: 01/04/23