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

Project name: AutoSpeedWatch System within Walton [Somerset]

Data controller(s): Walton Parish Council -Clerk

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)

SPEED CAMERAS

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)?

THE EXPANSION OF EXISTING CAMERA SYSTEMS UNDER THE GDPR

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.

CONTEXT: In locations within the parish [A39 Main Street] where there is a known and ongoing speed issue that is generating a safety threat and loss of amenity, and where Walton Parish Council has agreed the need for additional road safety measures as part of the Walton Community Speedwatch local police force team.

PURPOSE: To only capture images of vehicles [not individuals] that are speeding significantly above the notified speed limit such that enforcement authorities can take the action they feel appropriate to improve the road safety at that location.

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/

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?

NATURE: There is no personal information being processed. Vehicle registration numbers are not classified as personal information. No individuals are captured, and if accidentally captured any associated records are removed from the system as part of usage policy.

SCOPE: No personal data. Vehicle image, vehicle registration number, date, location and time. MoT and tax status.

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 vehicle registration number and associated data is transferred to the local police force who decide whether the vehicle is causing an actionable threat to safety. The data is passed in one direction only. Action decisions are not made within Autospeedwatch Limited but by the police. Usage terms and conditions prevent the use of the information collected for any purpose other than for road safety management.

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)

Fixed position, fixed field of view, speed activated camera.

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.

From camera to secure server managed by AutoSpeedWatch Limited.
From secure server to Police force.
No surveillance technologies used, and no faces recorded for recognition.
Records are deleted automatically according to the data retention policy.

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.

Individual still images are recorded to AutoSpeedWatch server. No audio

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)

By direct access to images on the AutoSpeedWatch server via known police user registered access.

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)

Non-image data associated with image [speed, vehicle registration number, location, date, time etc.] sent to police by email report.

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
Parishioners	Representation by elected Councillors for the parish	general recognition of need for further traffic calming measures. Speed of traffic hazardous. Existing signage considered not sufficient. Existing speed indicator device at edge of village considered not sufficient.	autospeedwatch system
Property owners of any property within field of view camera	Councillor/property owner conversation as required.	none	No properties within field of view
Community Speedwatch group	councillor/ community Speedwatch team liaison	location in centre of village requested.	Site of AutoSpeedWatch unit agreed in liaison with Community Speedwatch group.

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.

Parish and community duty to work with the police in the management of road safety risks as part of the community Speedwatch team. The SCC commissioner has confirmed that such systems, correctly applied, for support of the police are acceptable.

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.

Use of informed consent signage, with contact information.

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?

The system is in a fixed position and triggers capture only for the purposes of recording speeding vehicles. This function cannot be changed by any user, nor can the unit be redeployed for any other function. Should roadside units get stolen they are reported as such and can be disabled by AutoSpeedWatch Ltd. In such a way that they cannot be re-enabled independently.
The proportion of speeding is logged and the system can be disabled when the local authority review assess that it is no longer needed.

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

No more than 365 days according to company data retention policy. Records can be deleted before this. Data is automatically deleted and once deleted there is no recovery.

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)

Automated script removed the images and associated data at 365 days. Meta data [count of records deleted is kept indefinitely.

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?

Each roadside unit camera is built by design to be secure from unlawful / malicious attack. Communications between subsystem on devices encoded. ~Images are not stored locally, but transmitted in encrypted form for storage on Autospeedwatch Ltd. centralised server. Data is only accessible to registered and approved users, who cannot re-write, edit or manipulate data by virtue of inherent permissions. The lead user [coordinator role] is assigned by this parish and is responsible for managing operational use. That coordinator can add other members [validators and readers] with limited access rights to assist in operation. Each member must agree to the Autospeedwatch Ltd. terms and conditions of use to gain access.

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.

By reference to the parish policy document. As no images where a subject appears are kept there should be no image release mechanism required. The policy describes a process for how enquiries are handled.

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.

Walton village Main Street is the A39 there have been a number of road traffic accidents. The parish council has supported the existing traditional Community Speedwatch team; however they cannot maintain a continuous presence. The community Speedwatch team suggested the Autospeedwatch system as a practical addition due to the number of speeding vehicles they had been recording.
There is an existing Fixed vehicle activated device that has been in place for many years and is located at one end of the village to remind about the speed limit upon entry of the village but it is unable to create an impact throughout the centre of the village. Road small improvement schemes to reduce speed are not financially available at this time and due to the nature of the A39 [narrow with narrow

pavements and with significant HGV usage] may not be deemed appropriate for this location. Due to the presence of lamp posts, repeater signs are not in place along Main Street. One mobile speed indicator device is in use around the village in order to increase the general awareness of the speed limit, however data collated from that device indicates that there continues to be speeding through the village, data from this device along with data provided by the Autospeedwatch unit itself would be used to assist in indicating if the continued presence of the Autospeedwatch system was required. Council considered that the Autospeedwatch system that could link in with the police and support the work of the community Speedwatch team, would be most appropriate at this time due to the existing speed management not being sufficiently effective.

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)

Walton Parish Council Autospeedwatch Camera policy.

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** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
Homes / dwellings – viewing of personal habitation space.	Remote	minimal	Very low
Capture of faces within image of rear view of vehicle	Remote	minimal	Very low
Storage of image data longer than necessary	Remote	minimal	Very low
Copying or distribution of images by users	possible	minimal	Very low
Public not informed of camera usage	possible	minimal	low

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** *Eliminated reduced accepted.*	**Residual risk** *Low medium high*	**Measure approved?** *Yes/no*
Request disabling of camera where privacy invasion risk is changed and considered inappropriate.	eliminated	low	yes
Reposition camera	reduced	medium	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 [data protection officer] 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: for annual review		
This DPIA will be kept under review by: The Parish Clerk and Council Chairman		The DPO should also review ongoing compliance with DPIA.

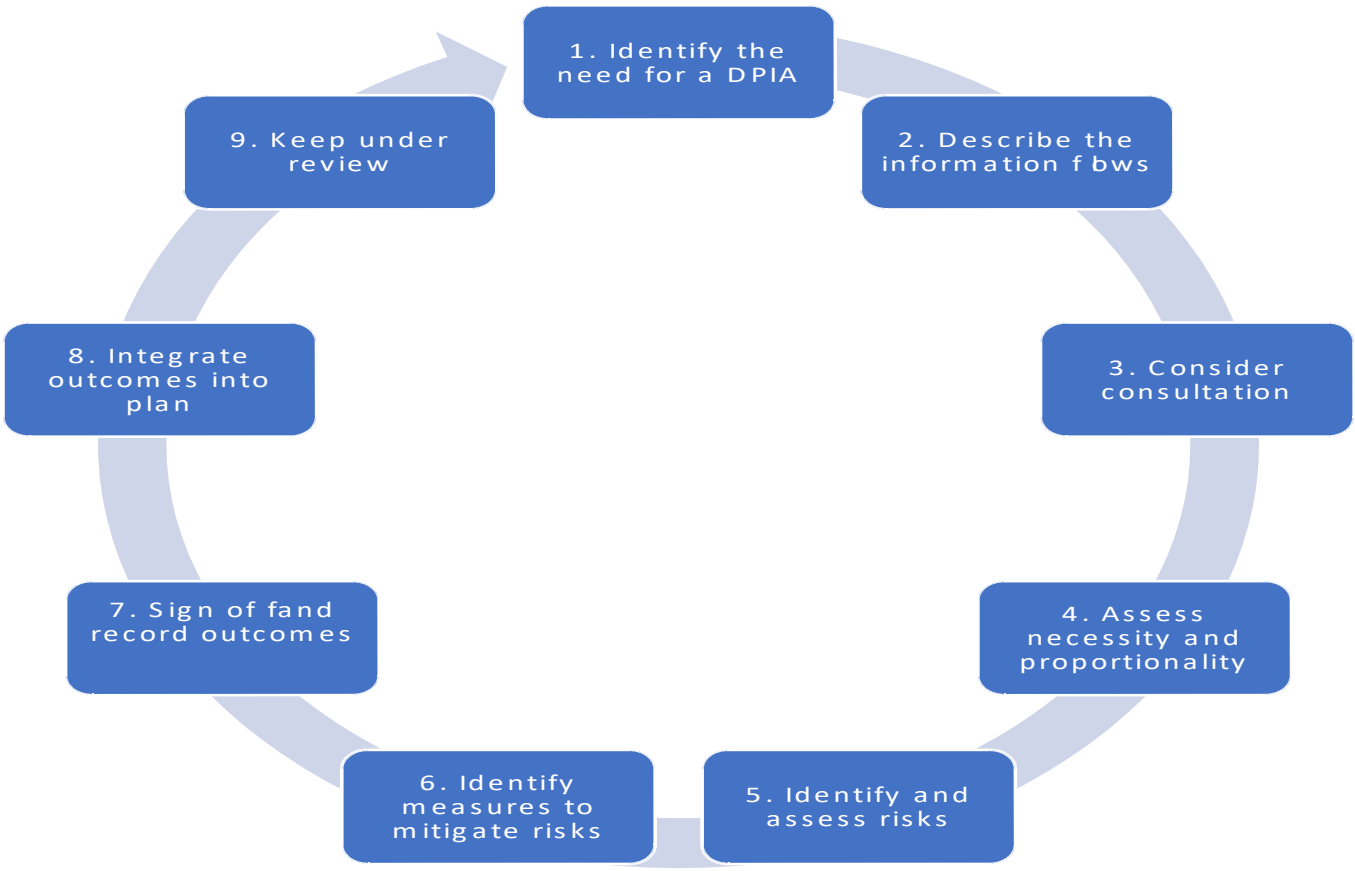
APPENDIX ONE

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)
A39 directly outside the old school building	ASWRU01	1	Daylight hours only	Only speeding offences, reviewed by registered community Speedwatch team member at a later date.	No specific mitigations

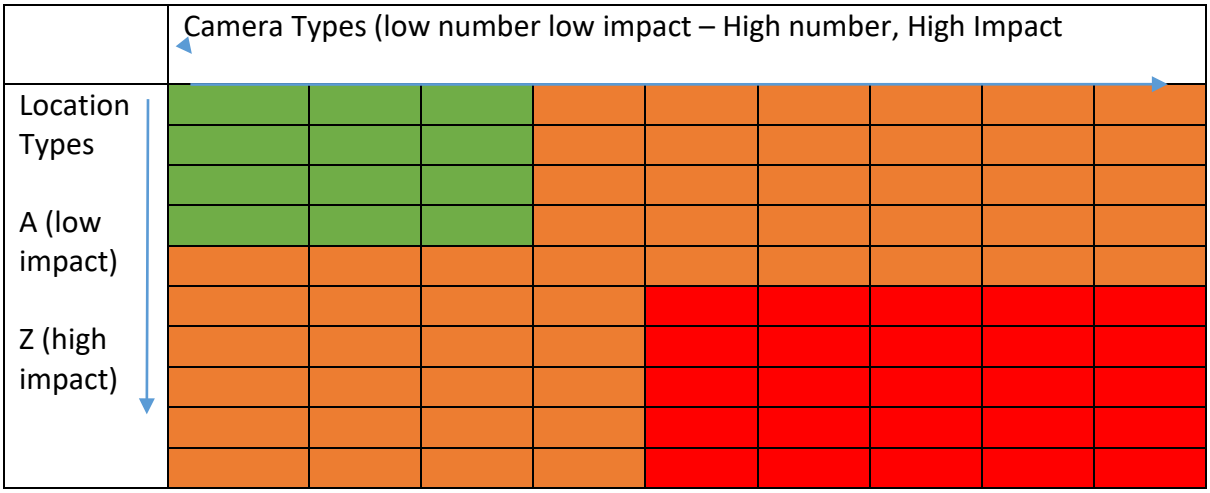
APPENDIX TWO: STEPS IN CARRYING OUT A DPIA



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:



NOTES

Date completed: <date>