

Data protection impact assessments

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



Project name: Birdlip Parish Council CCTV

Data controller(s): Elaine Lavington (Clerk) and Oliver Hale (Councillor)

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 DPIA¹:

- | | |
|---|---|
| ☐ 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) |

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)?

New deployment protected under DPA 2018

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 including ANPR Camera installed throughout Birdlip specifically at the entrances to the village.
Purpose;

1. Crime Prevention
2. Keep our residents safe
3. Assist Police with the apprehension of offenders of Crime and Antisocial Behaviour

The Local Government and Rating Act 1997 s31 allows a Parish Council the ability to spend on crime detection and prevention measures in it's area. The lawful basis for collecting the data via CCTV and ANPR is classed as public task and necessary as there is no other safe way to gain evidence of anti-social behaviour.

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/>

The processing will be targeted and a proportionate way of achieving BPC's goals purpose.

The data will not be kept longer than necessary (30 days)

BPC has a Model Publication Scheme Policy, IT Acceptable usage and Data Protection Policy which explains to individuals their rights to data and the responsibilities of the council. All policies are regularly reviewed.

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?

CCTV will be unmonitored. Recordings of road users, vehicle and pedestrians will be held for 30 days and then automatically deleted.

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 operatives of the system are from Birdlip Parish Council these are the clerk, and a Parish Councillor, who will be trained on the reviewing and recording of the data. Data recordings will not be accessed unless a request has been received and processed in accordance with Birdlip Parish Councils CCTV and Data Protection Policies.

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 collected will be unmonitored. Automatic deletion will take place after the retention period.

The footage captured by the cameras situated at entrances to and from the village of Birdlip are transmitted using a wireless transmitter to a Network Video Recorder (NVR) drive recorder undisclosed location. These recordings are overwritten in a loop every 30 days. Any approved recordings are taken from the NVR via memory stick and delivered / collected by hand to ensure receipt. Any requests for viewing of the data is logged by the reviewer with the action taken. All such requests are fully logged.

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.

Recording is undertaken in a locked specialist cabinet, at undisclosed location. Cameras are not enabled for 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)

Copies of footage will be released to either an individual who has requested a copy of their personal data or to authorised agencies to aid the evidence of a crime / find individuals. The images will be downloaded onto a memory stick and either collected or hand delivered.

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)

Upon request by an individual for their personal data

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
Residents	Social Media - Whatsapp groups Facebook groups	Positive in favour Will system be monitored	System not monitored
Residents	Annual Village meeting	Positive in favour Will system be monitored	System not monitored
School Governors	Governors Meeting	Will CCTV and appropriate Data protection systems and policies be in place.	All policies to be in place before CCTV goes live.
Residents	Questionnaire	None	None

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.

Under section 17 of the Crime and Disorder Act 1988 a local council has a duty to: exercise its various functions with due regard to the likely effect of the exercise of those functions on, and the need to do all that it reasonably can to prevent,

- crime and disorder in its area (including anti social behaviour and other behaviour adversely affecting the local environment

- the misuse of drugs, alcohol and other substances in its area

and; - re-offending in its area In addition Section 31 of the Local Government and Rating Act 1997 permits a local council, in order to prevent or detect crime to:

- install and maintain any equipment

- establish and maintain any scheme, or

- assist others to install and maintain any equipment or to establish and maintain any scheme.

The Law Enforcement Directive (LED) enables the Council to process personal information without some of the normal safeguards required by the General Data Protection Regulations. LED controls the processing of personal data where it relates to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against, and the prevention of threats to public security. The Council will also use CCTV camera systems under Section 163 Criminal Justice and Public Order Act 1994.

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.

Signs will be placed on the approach to and exits from the village of Birdlip

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 cameras work 24/7 and will record all activities occurring within their viewing capacity. The viewing of this data will only occur when requested by appropriate and authorised authorities. We will know that it is delivering the benefits by the reduction in incidents reported to the police and by reports from the groups on the reduction of incidents occurring.

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

30 days - the NVR works on a continuous loop recording over itself after the 30 day period - the retention period of 30 days is considered a long enough period for any approved authorities to contact the Council to ask for the images to be reviewed to support any crime issues

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)

If the police or relevant agencies require the footage it will be downloaded onto a memory stick and saved until they require it.

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?

The NVR system is situated in a locked purposed built cupboard. Only the Data Controllers have the details of how to access the system. All recordings downloaded on memory stick will be kept safe until collected or delivered by hand. The system is password protected. Upon an approved request for the Council to view the recordings, if evidence is found (or personal data is found) the images will be downloaded onto a memory stick. The person will either collect the memory stick (showing proof of ID) or the Clerk or Councillor will hand deliver the memory stick (again asking for proof of ID) We will not transfer data internationally.

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 Parish Council anticipates that CCTV coverage will, in most instances, only be made available directly to Gloucestershire Constabulary. All crime should be reported to the Police and they will access the footage if required.

In other exceptional circumstances, residents and public may make a request for CCTV footage and should do so only with reference to the 'Birdlip CCTV Policy', Those making the request will need to

provide proof of identity. There is a small charge for a data request to be considered. Any members of the public not directly involved in the request will have their identity masked.

The council recognises that individuals whose information is recorded have a right to be provided with that information or, if they consent to it, view that information. Requests will be dealt with promptly. It should be noted that Individuals will only have a maximum of 14 days to make a request before the footage is automatically deleted. All requests are subject to operational considerations for example where; - Footage has been requested by and/or passed to the Police as part of an investigation of a crime; or - Footage has been requested in respect of a road traffic collision and the information has been passed to insurers; or - Any relevant exemptions. The individual will be asked to supply an up to date photographic ID of themselves to enable the operator to identify the person on any recordings and any approximate times that they may have been recorded to assist with the viewing.

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.

The camera operation needs to be continuous to enable the detection of crime. No other options to date have been successful in combating antisocial behaviour and Crime prevention.

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 policies and procedures will be assessed at least annually by the Parish Council. An internal auditor reviews processes and policies on an annual basis of which this is included. We have an annual maintenance contract with the supplier who verifies and upgrades the system as required.

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
General public including children and vulnerable adults will be captured on surveillance recordings. No long term retention of footage.	Remote, possible or probable Possible	Minimal, significant or severe Minimal	Low, medium or high Low
Residents privacy. Specific areas of capture can be masked at the request of the householders, where cameras overlook residential properties and businesses.	Possible	Minimal	Low
Data Breach – Should data protocols be breached data could be stolen and used by those unauthorized to do so. All systems are encoded to prevent data from being hacked. Staff trained how to use systems correctly in line with policies.	Possible	Minimal	Low
Electrocution: Members of the public could touch live wires Hardware installed by a competent contractor. Inspection is completed on a monthly basis	Possible	Minimal	Low

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
Length of time the recordings are retained - if the recording fails, this could lead to a false sense of feeling safe when in the area covered - mitigation is to perform a weekly check to ensure system is working effectively.	Remote, possible or probable Remote	Minimal, significant or severe Minimal	Low, medium or high Low
Sharing of recordings - the CCTV policy and procedures mitigate the risk of inappropriately sharing the recordings	Remote	Minimal	Low
Intrusion - the Signage and policies clearly state that there are cameras in operation. The cameras will not intrude onto any private property - if the camera's are moved, we will ensure that the cameras are configured to black out the part of the image that contains windows.	Remote	Minimal	Low
The only operatives of the system are the clerk and nominated Councillor. They have been trained and have agreed to abide by the CCTV policy and procedures. Any wrongdoing by them would result in disciplinary action.	Remote	Significant	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	Residual risk	Measure approved?
All Data Administrators will complete training and will have a clear understanding of the CCTV and GDPR procedures. Training by the CCTV Supplier - full training is provided as part of the installation of the system	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
Privacy masking will be undertaken for affected residential properties at the householders request	Eliminated	Low	Yes
Pre-purchase of Memory Sticks - to ensure that if an approved request is made for images from the system, memory sticks are available to record the data onto.	Eliminate	Low	Yes

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Damage to any of the system- the supplier will be contacted and the system will be fixed - the council will pay for a maintenance contract	Eliminated reduced accepted Accepted	Low medium high Low	Yes/no 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: Birdlip Parish Council		Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by: N/A		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: Parish Clerk		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: Parish Clerk		If your decision departs from individuals' views, you must explain your reasons.
Comments:		

This DPIA will be kept under review by: Parish Clerk		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)
Residential Street within the Village of Birdlip	Recording	9	24hrs	Periodic inspection to ensure all are working. Not monitored - only viewed where appropriately requested	ASB ongoing problems - to assist with evidence of crime / asb CCTV areas have clear signage stating its use and purpose with our contact details
Residential Street within the Village of Birdlip	ANPR	2	24hrs	Periodic inspection to ensure all are working. Not monitored - only viewed where appropriately requested	As above

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:

		Camera Types (low number low impact – High number, High Impact)							
									
Location Types A (low impact) Z (high impact)									

NOTES

All cameras and recorders, designed to capture images of people and cars which would enable appropriate authorities to identify individuals / vehicles. The residual risk factor for all cameras is Low.

