



**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:** Sabden Parish Council CCTV Cameras

**Data controller(s):** Karen Buckley, Mark Dawson & Claire Clapham

**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<sup>1</sup>:**

- |   |   |
|---|---|
| <input type="checkbox"/> Systematic & extensive profiling | <input type="checkbox"/> Large scale use of sensitive data        |
| <input checked="" type="checkbox"/> Public monitoring     | <input type="checkbox"/> Innovative technology                    |
| <input type="checkbox"/> Denial of service                | <input type="checkbox"/> Biometrics                               |
| <input type="checkbox"/> Data matching                    | <input type="checkbox"/> Invisible processing                     |
| <input type="checkbox"/> Tracking                         | <input type="checkbox"/> Targeting children / vulnerable adults   |
| <input type="checkbox"/> Risk of harm                     | <input type="checkbox"/> Special category / criminal offence data |
| <input type="checkbox"/> Automated decision-making        | <input type="checkbox"/> 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)?

We have 4 camera's within Sabden Parish. One installed on the Ribble Valley Car Park, Padiham Road. A camera on The White Hart Pub Padiham Road Sabden, and one on Ella Mia Beauty Salon Whalley Road. The camera's will comply General Data Protection Regulations (GDPR) and the Data Protection Act (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.

The main reason is to support Lancashire Police Rural Task Force whos aim is to target rural communities where there has been an increase in machinery theft, rural, wildlife and heritage crime Sabden is central within the Ribble Valley and many vehicles will pass through the village from the A59. The camera's will also:

Support detection and investigation of anti-social behaviour and criminal activities.  
Reduce the fear of crime and anti-social behaviour.

<sup>1</sup> <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/>

Support the police to prevent and detect crime.  
 Reducing vandalism and graffati.  
 Improving the safety and security of residents and visitors of Sabden.  
 Assisting in identifying, apprehending, and prosecuting offenders.  
 Supporting Traffic Enforcement under the legislation: The Road Traffic Act 1988 and The Traffic Management Act 2004.

Although Sabden generally has a low crime rate, recently there has been incidents of burglary and vandalism to the childrens play area. There has also been house burglaries and several attempts to steal cars.

Ribble Valley crime figures have increased over the last 3 years the latest figures and percentage increases are stated below:

Anti-social behaviour	253	31.5%
Burglary	69	8.6%
Criminal damage and arson	60	7.5%
Other theft	83	10.3%
Possession of weapons	3	0.4%
Public order	31	3.9%
Shoplifting	5	0.6%
Violence and sexual offences	208	25.9%
Other crime	21	2.6%
Drugs	15	1.9%
Robbery	1	0.1%
Theft from the person	4	0.5%
Vehicle crime	48	6%
Bicycle theft	3	0.4%

**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?

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 31 days after which there is an automatic deletion of the footage, unless required for criminal investigation and/or prosecution.

The processing of the data will be proportionate to the achieving of the purposes listed.

**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 will be accessed for permitted reasons only by authorised personnel from Sabden Parish Council. The data will be shared for the purposes of crime prevention and prosecution to the following bodies:

- Law enforcement agencies where footage recorded would assist in a criminal enquiry and for the prevention of disorder.
- Relevant legal representatives
- People whose images have been recorded and retained unless disclosure would prejudice criminal enquiries or proceedings.
- Emergency services in connection with the investigation of an accident

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)**

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Fixed CCTV (networked) | <input type="checkbox"/> Body Worn Video                  |
| <input type="checkbox"/> ANPR                              | <input type="checkbox"/> Unmanned aerial systems (drones) |
| <input type="checkbox"/> Stand-alone cameras               | <input type="checkbox"/> Redeployable CCTV                |
| <input type="checkbox"/> 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.

There is no automated facial recognition technology or audio recording.

The retention periods is 31 days after which there is an automatic deletion of the footage unless required for criminal investigation/prosecution.

Authorised personnel have received relevant training in legislation, procedures and use of the system.

Footage may be retained securely for more than 31 days for investigation or a subject access request. Unless exceptional or unique circumstances apply, this data will be manually deleted after 12 calendar months. The system is reviewed by a 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.

CCTV Server room contained within secure CCTV Control room and 2 recording boxes both within secure buildings.

#### 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 prescribed and access passwords will be sent separately 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)

## Consultation

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

<b>Stakeholder consulted</b>	<b>Consultation method</b>	<b>Views raised</b>	<b>Measures taken</b>
Ribble Valley Council	Parish Council meetings.		
Lancashire Constabulary Rural Police	Meetings and on site visit.		
Residents of Sabden	Leaflet drop to all residents and invite to Sabden Parish Council meeting.	Concerns over invasion of privacy	Sabden Parish Council policies and procedures clearly specifics how footage will be monitored and used. This will shared on Sabden Parish Council website.

--	--	--	--



## 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 Sabden Parish Council as a competent authority to process personal 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 official authority vested in the controller.

Sabden Parish Council in conjunction with Lancashire Constabulary are working together to facilitate the lawful exchange of information to work together to develop and implement a strategy and tactics for reducing crime and disorder, anti social behaviour and rural crime. 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.

Legislation also includes - The Road Traffic Act 1988 and The Traffic Management Act 2004.

**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.

Sabden Parish Council will publish the DPIA for transparency also Sabden Parish Council CCTV policies and procedures will be displayed on our website.

Public consultation at Parish Council Meeting

Appropriate signage in and around the area where surveillance is taking place.

**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?

Sabden Parish Council has installed CCTV cameras around the village 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.

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 Sabden Parish Council must be able to provide the police with evidence to enable criminal proceedings.

Some examples of how we use the data are provided below;

- Providing evidence in criminal proceedings (police and criminal evidence act 1984 and criminal procedure and investigation act 1996)
- 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.

Effectiveness of the system along with compliance with the Protection of Freedoms Act 2012.

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)

There are no laws that sets out a timeframe for retaining CCTV. Sabden Parish Council in line with guidance have agreed to store data for a maximum of 31 days. 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. 31 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 securely for more than 31 days where required for an investigation or subject access request.

Date and version control: 19 May 2020 v.4

**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.

If required encrypted USB are released to third parties such as, police and email confirmation prior to disclosure of the encryption code.

**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.

Sabden Parish 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 Sabden Parish Council website. Any complaints are dealt with through the councils complaints procedures and should be emailed to [clerk@sabdenparish.org.uk](mailto:clerk@sabdenparish.org.uk).

**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 currently used within the village but is not a solution to detect or prevent anti social behaviour. An increased presence of police is requested but not always available.

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

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 authorised personnel.

## 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.

<b>Describe source of risk and nature of potential impact on individuals.</b> Include associated compliance and corporate risks as necessary.	<b>Likelihood of harm</b>	<b>Severity of harm</b>	<b>Overall risk</b>
<p>Compliance with articles of the Human Rights Act;</p> <p>The Act applies to public authorities and other bodies, which may be public or private, when they are carrying out public functions</p> <p>Article 6: the right to a fair trial            Article 8: right to a private and family life            Article 14: protection from discrimination</p> <p>A breach of any article may impede on the subjects rights and result in the prosecution of the parish council resulting in financial penalties and severe damage to its reputation</p>	<p>Remote, possible or probable            Possible</p>	<p>Minimal, significant or severe            Significant</p>	<p>Low, medium or high            Low</p>

Security of Data. A Security Data breach may result in prosecution under GDPR/DPA 2018 and result in financial penalties and severe damage to the reputation of the parish council.	Possible	Significant	Low
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: <ul style="list-style-type: none"> <li>• Lawfulness, fairness and transparency</li> <li>• Purpose limitation</li> <li>• Data minimisation</li> <li>• Accuracy</li> <li>• Storage limitation</li> <li>• Integrity and confidentiality (security)</li> <li>• Accountability Non compliance may result in prosecution, financial penalties and severe damage to the reputation of Sabden Parish Council</li> </ul>	Possible	Significant	Medium
<b>Describe source of risk and nature of potential impact on individuals.</b> Include associated compliance and corporate risks as necessary.	<b>Likelihood of harm</b>	<b>Severity of harm</b>	<b>Overall risk</b>
Unauthorised Disclosure Unauthorised Disclosure may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the parish council.	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Low
Misuse of Data Misuse of data may result in prosecution under GDPR/DPA 2018 and subject to financial penalties and severe damage to the reputation of the parish council.	Possible	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.**

<b>Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk</b>			
<b>Options to reduce or eliminate risk</b>	<b>Effect on risk</b>	<b>Residual risk</b>	<b>Measure approved?</b>
Compliance with GDPR/DPA 2018. Management of the use and security of the system including monitoring and downloading of footage. Regular audits carried out.	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 authorised personnel.	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. Checks on proactive monitoring by authorised personnel and use of passwords to protect data.	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes
<p>Unauthorised Disclosure Release of data is strictly controlled by the parish council.</p> <p>All personnel who use data from the system are aware of their obligations under GDPR/DPA.</p> <p>Full audit trail for any release of data. CCTV authorised personnel trained in unauthorised disclosure and misuse of data.</p>	Reduced	Low	Yes
Misuse of Data Release and use of data is strictly controlled by the parish 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 authorised personnel trained in unauthorised disclosure and misuse of data.	Reduced	Low	Yes
Financial Loss. Compliance with GDPR/DPA, following code of Practice and operating procedures reduces the risk of unauthorised disclosure or the misuse of data. Regular audits are carried out by authorised personnel.	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.

<b>Item</b>	<b>Name/date</b>	<b>Notes</b>
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:		

Date and version control: 19 May 2020 v.4

This DPIA will be kept under review by:		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 type	Monitoring	Assessment of use of equipment (mitigations or justifications)
Ribble Valley Car Park. Padiham Road		1	24hrs destroyed after 31 days	No routine monitoring. Access required as set out in Sabden Policy and Procedures document.	The privacy level expectation in a village centre is very low; there is CCTV signage warning residents that they are being recorded.
The White Hart Padiham Road Sabden		2	24 hrs destroyed after 31 days	No routine monitoring. Access required as set out in Sabden Policy and Procedures document.	The privacy level expectation in a village centre is very low; there is CCTV signage warning residents that they are being recorded.
Ella Mia Whalley Road Sabden		1	24 hrs destroyed after 31 days	No routine monitoring. Access required as set out in Sabden Policy and Procedures document.	The privacy level expectation in a village centre is very low; there is CCTV signage warning residents that they are being recorded.

## 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

Date and version control: 19 May 2020 v.4

