



**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:** Holbeach Parish Council Public Space CCTV

---

---



**Data controller(s):** Holbeach Parish Council

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

**1. Identify why your deployment of surveillance cameras requires a DPIA<sup>1</sup>:**

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

Public space, Carters Park monitoring for crime prevention, detection of crime and public safety. For the security of Carters Park and safety of staff.

**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)?

This is a new system which is monitored & maintained in accordance with the SCC Code of Practice and governing guidance. Holbeach Parish Council has a statutory duty under the Crime & Disorder Act 1998, Section 17 to prevent and deter crime and disorder. In addition as a local authority we have responsibilities for public safety and safeguarding and processing is undertaken under Article 6(1) (e) of the GDPR / Schedule 2, DPA 1998 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.

Holbeach has faced challenges of crime and disorder in the past and the surveillance camera system has been designed to address these issues. In 2022 there was a marked increase in anti-social behaviour and crime within the park. The aim of the CCTV is to make a visible long-term contribution to

<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/>

improving the quality of life to those who work and visit the park and CCTV is integral for this and also enhances community confidence and reduces the fear of crime.

CCTV cameras have been installed in Carters Park to assist in the prevention and detection of crime, improve public safety and reduce anti-social behaviour..

**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 Carters Park. The data collected and processed is in the form of recorded video footage. There will be images of children, vulnerable persons, people from minority ethnic groups and religious beliefs however this will not be known at the time of recording unless the cameras are being proactively used by staff.

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

The CCTV system, does not discriminate in any way, nor does it have any analytical software which could be used to discriminate people.

**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.

Holbeach Parish are the system owners. The Surveillance Code of Practice includes details in relation to data sharing agreements and when data can and can't be shared. The lawful basis for processing is to enable us to carry out our public task functions as set out in the Crime & Disorder Act 1998.

The council will share data with

1. Data subjects
2. Statutory prosecuting authorities
3. Clients and authorised investigators

There will be a Data Sharing Agreement with Lincolnshire Police that is being reviewed.

No other organisation will have access to the data other than general individuals exercising their rights in relation to subject access requests.

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

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

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

Data will be captured in video format. The system is hard wired. The retention period is 31 days after which there is an automatic deletion of the footage. Procedures, data sharing and security are in line with Council policy and procedures. Authorised staff have received relevant training in legislation, procedures and use of the system. Footage may be retained in an evidence locker for more than 31 days. e.g. major incident where a large amount of data has been retained for investigation. Civil Proceedings and Subject Access Requests. The evidence locker is reviewed by the manager on a monthly basis. The principles of GDPR/DPA 2018 will be adhered to at all times.

1. Live video images collected real-time by CCTV cameras.
2. Live video images stored securely, no integrated surveillance technologies will be used.
3. All live video recordings will be stored, but not accessed or reviewed until necessary or requested. this will be undertaken by trained and qualified staff.
4. All CCTV footage to be deleted after 31 days in line with guidelines on a rolling basis

**8. Does the system's technology enable recording?**

- Yes                       No

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

Local Authority CCTV server room.

**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)

Officers will attend in person - will require documentation and signing over to accept responsibilities as the data controller.

Subject Access Requests, requests from Insurance Companies and solicitors will be dealt with by using encrypted media and courier or recorded delivery. All parties are required to sign a disclosure form for any media.

**10. How is the information used? (tick multiple options if necessary)**

- 
- 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>
Elected Members	Full Council meeting	In favour	
Lincolnshire Police, Holbeach	Site visit	Fully supportive, used to locate wanted persons, sexual assault offender identification, locating missing people and monitoring ASB in and around Carters Park	

Date and version control: June 2023 v.1

## **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 official authority vested in the controller. There will also be at times processing necessary in order to protect the vital interests of the data subject for matters of life or death. The CCTV system established by Local authorities is under the GDPR/DPA 2018 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.

Section 17 outlines the reasonable actions that can be put in place to ensure a co-ordinated approach to crime reduction. 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.

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.

Where there are surveillance camera systems display signage around the facility, making all visitors and staff aware the system is live and in 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?

Footage will be stored on site in a secure and restricted access room. Access will only be available to trained staff with designated authority to do so.

The installation of CCTV (Closed Circuit Television) cameras in various locations within the park is 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 visit and work in the park.

The purpose and use of the CCTV system is 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.

Date and version control: June2023 v.1



In all locations, signs are displayed notifying that CCTV is in operation  
Effectiveness of the system is measured in monthly performance indicators along with information supplied by the police.

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

Video images will be stored for 31 days in line with legislation, this will then be automatically over ridden by more recent footage. If needed to be retained the footage is transferred into a secure folder and not kept for longer than is necessary.

### 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 for more than 31 days, the secure file is reviewed by the manager on a monthly basis.

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

The data will be stored on a hard drive, with the technology to automatically override the video footage when out of the 31 day period. The system is stand alone but will meet all of the councils necessary ICT safeguarding restrictions to ensure it complies. The hardware and system access will only be accessible by trained and authorised staff (Clerk & Deputy Clerk). The data room is secured by lock and key with only the Clerk & Deputy Clerk having access to the key which is stored off site. The disclosure of images is controlled and in accordance with the CCTV Code of Practice.  
DVD's / encrypted USB are released to police officers, third party releases such as Insurance companies and solicitors are undertaken via recorded delivery and no international transfers are made.

**18. How will you respond to any subject access requests, the exercise of any other rights of data subjects, complaints or requests for information?** Explain how you will provide for relevant data subject rights conferred under the legislation. You must have procedures in place to respond to requests for camera footage in which a subject appears, and to respond to any other request to meet data protection rights and obligations.

A subject access request (“SAR”) must be a written request from an individual to obtain a copy of the information the Council holds about him or her. As there are strict time periods for complying with a SAR (1 calendar month from the date of the SAR). The process and application form is set out in our Code of Practice and is also available on our website.

<https://holbeach.parish.lincolnshire.gov.uk/downloads/file/687/subject-access-requests-procedure>

Any complaints are dealt with through the councils complaints procedures.

**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 various locations are public areas.

Due to the need to detect crime and investigation of crime and for safeguarding there is no less intrusive option to deliver the same outcome. The cameras are recording constantly but are not directed at individuals. Privacy zones are utilised along with regular training and audits.

**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)

There is monthly audit by the CCTV Supervisor (Clerk) in relation to footage disclosed to the Police .  
There is a CCTV 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	Severity of harm	Overall risk
<p>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:</p> <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</li> </ul> <p>Non compliance may result in prosecution, financial penalties and severe damage to the reputation of the local authority</p>	<p>Remote, possible or probable Possible</p>	<p>Minimal, significant or severe Significant</p>	<p>Low, medium or high Medium</p>

<p>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</p> <p>Article 6: the right to a fair trial</p> <p>Article 8: right to a private and family life</p> <p>Article 14: protection from discrimination</p>	Possible	Significant	Medium
<p>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</p>			
<p>Compliance with SC Code of Practice and the Protection of Freedoms Act 2012.</p> <p>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.</p> <p>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.</p> <p>The surveillance camera code is admissible in evidence in any such proceedings.</p> <p>(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</p> <p>Reputational damage to Local Authority. The court may take inference in an authorities non compliance.</p>	Possible	Significant	Medium

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 local authority	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 local authority	Remote, possible or probable Possible	Minimal, significant or severe Significant	Low, medium or high Medium
Misuse of Data Misuse of data may result in prosecution under GDPR/DPA 2018 and subject to financial penalties 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.**

<p><b>Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk</b></p>	
--	--

<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, reviewing 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, reviewing and downloading of footage. Regular audits carried out and spot checks proactively monitoring staff.	Reduced	Low	Yes
Compliance with SC Code of Practice and the Protection of Freedoms Act Management of system.	Reduced	Low	Yes
<b>Options to reduce or eliminate risk</b>	<b>Effect on risk</b>	<b>Residual risk</b>	<b>Measure approved?</b>
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	Eliminated reduced accepted Reduced	Low medium high Low	Yes/no Yes

<p><b>Security of Data</b>  Management of the use and security of the system including monitoring, reviewing and downloading of footage. Regular audits carried out. Proactive monitoring by staff, use of passwords and checks carried out by maintenance contractors for network security.</p>	Reduced	Low	Yes
<p><b>Financial Loss.</b>  Compliance with GDPR/DPA, POFA, Code of Practice and operating procedures reduces the risk of unauthorised disclosure or the misuse of data. Regular audits are carried out by the CCTV Supervisor.</p>	Reduced	Low	Yes
<p><b>Misuse of Data</b>  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.</p>	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:	Holbeach Parish Council	Integrate actions back to HR, H & S and Data Protection Committee
Residual risks approved by:	Holbeach Parish Council	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:	Jan Hearsey – Clerk Holbeach Parish Council	DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice : Confirmation of compliance and that processing can proceed		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by: Chair of Holbeach Parish Council		If your decision departs from individuals' views, you must explain your reasons.

This DPIA will be kept under review by: HR, H & S and Data Protection Committee		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)
Carters Park	PTZ		24hrs (calendar month)	Limited due to the HD cameras on the walkways and roadside covering some entrances and exits of the Park	The privacy level expectation in this area is low. The areas are signed and provide contact details. used for crime purposes and high volume of asb, historically and criminal damage to equipment. For public safety and fear of crime.

## 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	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Types	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange	Orange
A (low impact)	Green	Green	Green	Orange	Orange	Orange	Orange	Orange	Orange	Orange
Z (high impact)	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red
	Orange	Orange	Orange	Orange	Red	Red	Red	Red	Red	Red

**Risk assessment**

Location	Cameras
Carters Park, Park Road, Holbeach	Green

Low impact	Medium impact	High impact
------------	---------------	-------------

**NOTES**