



**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: Hartlebury Parish Hall and environs CCTV system

Data controller(s): Hartlebury Parish Council and Hartlebury Parish Hall Management Committee

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:

- | | |
|---|---|
| <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)?

This will be a new deployment of 13 CCTV cameras covering the Parish Hall, the surrounding car parks and petanque court, as well as the MUGA and tennis courts.

We will be processing data under the Data Protection Act 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.

Video will be recorded from all 13 cameras to help prevent and document any anti-social behaviour, vandalism and/or illegal activity in or around the Parish Hall and surrounding facilities. There have been multiple reports of drug/alcohol use (and possible sales), neighbour intimidation and verbal abuse, as well as vandalism and fouling. This system will act as a deterrent as well as recording footage of any of these activities that persist.

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?

We will be processing members of the public's personal data who use or walk through the MUGA, tennis court, playing field, playground or Parish Hall car park, petanque court and entrance, as well as three internal cameras in the hall. The images will be held for a maximum period of 30 days.

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 system will be jointly operated by the Hartlebury Parish Council (Council) and the Parish Hall Management Committee (Hall). The active controllers will include the clerk of the Parish Council, and two representatives, one each from the Council and the Hall who are all trained on the operation of the system. There will be one active DPO. The data will only be disclosed to the authorised agencies when requested for the purposes of evidencing crime or supporting their activities in searching for individuals. Individuals can request a copy of the CCTV data which contain their personal data. All acces to the NVR is logged on the device and includes all logins and all actions taken while logged in.

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.

The Network Video Recorder (NVR) for all cameras will be situated in a locked purpose-built cabinet inside the hall. The cameras in and around the Parish Hall are wired directly to the NVR. The cameras at the MUGA are transmitted using a wireless link. These recordings are overwritten in a loop every 30 days. these camera recordings do not include audio.

Any requested recordings that are approved for viewing 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 (no evidence found / memory stick provided). For public information requests there may be a charge for the memory stick.

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.

All recordings are made on an NVR situated inside the Parish Hall in a secure location. These recordings are video-only.

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)

An individual who has requested a copy of their personal data will be given a copy once it has been reviewed and approved by the DPO using ICO guidelines and advice. All requests must be made in writing (including email). Authorised agencies can access recordings to aid the evidence of a crime / find individuals. The recordings will be downloaded onto a memory stick and either collected or hand delivered with proof of ID.

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 if the request is deemed valid by the ICO.

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 (Hirers and visitors to the Parish Hall)	There were two Community Conversation events hosted by the Parish Council as well as the Parish Meeting. At these events residents expressed their views in support of CCTV. There have also been specific visits with parishioners who live opposite the areas to be surveilled who were also strongly for the project.	All were in favour of the installation of CCTV, hoping it will immediately act as a deterrent to ASB as well as curtail alcohol/drug activity and vandalism in the covered area.	This CCTV system
Police	The local Safer Neighbourhood Team (SNT) are fully supporting this project.	There are more than enough reports of ASB and possible crimes to warrant 24 hour CCTV coverage.	This CCTV system
Parish Hall Management Committee	Questionnaire to hall hirers and volunteers as well as online.	Awaiting details of their consultation	

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 and Hall 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 also uses 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.

The Joint Controllers:

- Have developed a CCTV Policy that describes in detail who has responsibility and accountability for all Public Space surveillance camera system activities including images and information collected, held and used.
- Will publish the locations of its CCTV cameras and other information relating to the CCTV system on their websites at the following addresses: www.hartlebury-pc.gov.uk and hartleburyparishhall.co.uk
- Will implement consistent CCTV signage policy. All areas where CCTV is in use will have clear, consistent signs exhibited to comply with the Data Protection Act; this is to advise people that they are about to enter an area covered by CCTV cameras or to remind them that they are still in an area covered by CCTV. The signs will also act as an additional deterrent. CCTV signs will not be displayed in areas which do not have CCTV cameras. Signs will carry the outline of a CCTV camera. The information on the sign will explain who runs them (Hartlebury Parish Council and Hartlebury Parish Hall) as well as contact information. The signs, position and the message will be large enough to enable people to easily read the information on it.
- 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 30 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.

Date and version control: 19 May 2020 v.4

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 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 will be situated in a locked purpose-built cupboard, in the Hall. The key for the cabinet is in a locked safe within the Village Hall and only the existing Hall representative and DPO have the details of how to access the safe. All recordings downloaded on to a memory stick will be kept in the safe until collected. The system is password protected. Upon an approved request for the Controllers to view the recordings, if evidence is found (or personal data is found), the images will be downloaded onto a memory stick by the DPO. The agency/person will either collect the memory stick (showing proof

of ID) or the Clerk or DPO Councillor will hand deliver the memory stick (again asking for proof of ID). All deliveries of footage will be recorded. We will not transfer data internationally. All access to the NVR is logged on the device and includes all logins and all actions taken while logged in.

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 Controllers recognise that individuals whose information is recorded have a right to be provided with that information. Requests will be dealt with promptly. It should be noted that Individuals will only have a maximum of 15 days to make a request to allow for reasonable time to retrieve the footage before it 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; Any relevant exemptions.

The individual will be asked to supply an up to date photograph of themselves to enable the DPO to identify the person on any recordings and any approximate times that they may have been recorded to assist with the retrieval. Any request must include a time-frame and reason for the request. Requests without valid reasons may be denied based on ICO advice taken at the time of the request.

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 detection of crime. Any system with a smaller area of coverage would leave portions of the property unprotected. given the number of complaints of anti-social behaviour and fouling in these areas CCTV is the onle viable option for protection.

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)

The CCTV policy will be reviewed and approved at least every 3 years by the Parish Council and ratified by the Parish Hall Management Committee. An internal auditor reviews processes and policies on an annual basis of which this is included. We will perform all maintenance and upgrades the system requires.

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
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 frequent checks during the working week of the system to ensure it is working effectively - it is not possible to currently carry out the checks at a weekend.	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 do not intrude onto any private property. If the cameras are moved, we will ensure that the cameras are configured to black out the part of the image that contains windows	Remote	Minimal	Low
Function Creep - the cameras will not be deployed elsewhere or have their area of coverage expanded outside the area of the hall or MUGA and tennis court.	Remote	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
The system can only be accessed via keys to the Key Safe in the Village Hall and the CCTV cabinet the key to which is kept in a locked safe. The NVR is password protected with separate accounts for each processor.	Remote, possible or probable Remote	Minimal, significant or severe Significan	Low, medium or high Low
The only direct access to the system will be by the DPO and Hall Rep. They have been trained and have agreed to abide by the CCTV policy and procedures. Any wrongdoing by them would result in disciplinary action. Any access to the system is logged and each person accessing the system has their own login. This insures all operations are logged properly and can be checked.	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?
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
Pre-purchase of Memory Sticks - to ensure that if an approved request is made for images from the system, memory sticks are available to transfer the data onto	Eliminated	Low	Yes
Damage to any of the system- the supplier will be contacted and the system will be fixed. All equipment has a 1 year warranty and after that period any maintenance will be on a per incident basis	Accepted	Low	Yes

Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved?
Power cuts are an infrequent but real issue, and the system must be able to record 24/7. The system will have UPS backup to mitigate this.	Eliminated reduced accepted Eliminate	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: Hartlebury Parish Council and Hartlebury Parish Hall Management Committee	2 July, 2024	Integrate actions back into project plan, with date and responsibility for completion.
Residual risks approved by: Not applicable		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, CALC and ICO		DPO should advise on compliance and whether processing can proceed.
Summary of DPO advice		
DPO advice accepted or overruled by: (specify role/title)		If overruled, you must explain your reasons.
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons.

Comments:

This DPIA will be kept
under review by:

The DPO should also review
ongoing compliance with DPIA.

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)
Parish Hall Internal	3	3	24hours	Periodic inspection to ensure all are working. Not monitored - only viewed where appropriately requested	Appropriate signage for CCTV its use and purpose with contact details.
Parish Hall Car Parks, petanque and surroundings	1, 2	8	24 hours	Periodic inspection to ensure all are working. Not monitored - only viewed where appropriately requested	Appropriate signage for CCTV its use and purpose with contact details
MUGA, Tennis Courts	1	2	24 hours	Periodic inspection to ensure all are working. Not monitored - only viewed where appropriately requested	Appropriate signage for CCTV its use and purpose with contact details

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	Orange	Orange	Orange	Orange	Orange	Orange
	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

NOTES

All cameras are HD resolution, 20 FPS, 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.

