Data Protection Impact Assessment : CCTV

Submitting controller details

Name of controller	North Horsham Parish Council
Subject/title of DPIA	CCTV (Roffey Millennium Hall) DPIA
Name of controller contact /DPO (delete as appropriate)	Sarah Norman - Clerk to the Council Roffey Millennium Hall Crawley Road Horsham, RH12 4DT

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

North Horsham Parish Council is a large-sized Parish Council which is responsible for three buildings (with associated car parks where appropriate) recreation grounds, open spaces, woodland, playgrounds, allotments and a range of community assets.

This DPIA has been prepared to identify any data protection risks arising from the use of CCTV installed at one of the Council's properties, Roffey Millennium Hall (RMH). No other assets/properties currently house any CCTV, but should this change in the future, further assessments would be required.

The processing involves the collection of video (not audio) from inside RMH and the immediate exterior, for the public benefit through the prevention and detection of crime and assist with the security of Parish owned buildings for use by visitors and staff.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The data, or images, are collected via fixed cameras located inside and in the entrance to RMH. No other equipment is involved in the collection of the data.

The data is stored on a local PC (backed up to physical server) and is only accessible by the Clerk and Deputy Clerk and is password protected. All staff, including the Clerk and Deputy Clerk, have undergone training in Data Protection.

The source of the data is the individuals themselves as it is their image.

The data is automatically deleted after 30 days unless it is downloaded in response to an incident, complaint or for disclosure.

The data will not be shared except in the following circumstances:-

- when required by law (e.g., to assist the police or other enforcement authorities in the investigation of crime)
- to support legal proceedings
- where disclosure is otherwise permitted under the Data Protection Act 2018

There is the potential for the processing to be identified as High Risk as it is blanket data collection of all staff and visitors to the building and could involve the capture of special category data, for example, where footage reveals health/disability information.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data, or images, are collected via 3 fixed cameras located inside and at the entrance to RMH. No other equipment is involved in the collection of the data, and no audio is picked up or recorded. The cameras only record footage from entrances to the building and corridors/communal areas and do not have viewpoints into the rooms for hire.

The cameras are recording 24 hours per day, collecting images from inside the building and the Council owned area immediately outside the front doors to the building. This is therefore a substantial amount of data collected, but the footage is only reviewed or retrieved where necessary following an incident or, for example, a request from the Police.

The system is not designed to specifically collect either special category or criminal offence data.

However, there is the potential for the capture of special category data, for example, where footage reveals health/disability information.

In the event of criminal activity, such as assault/robbery, criminal offence data would be collected.

Staff, visitors, hirers of the building, members of the public and contractors are all affected.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The individuals whose data will be captured will be Staff, visitors, hirers of the building, members of the public and contractors accessing RMH together with people immediately in front of the building.

Individuals have limited control over the capture of the data excluding not approaching the front doors or not entering the building.

Signage is located at the front of the building, visible from the exterior as well as internally to make everyone aware that CCTV is in operation, the reason for its operation and the Council's contact details.

There is the potential for children and vulnerable groups to have their data collected and this has been considered when assessing the necessity of the system, the security in place and retention protocols.

There are no prior concerns over the processing or security flaws.

CCTV is a well-established system that is often found in public places and buildings.

The Council is not signed up to any approved Code of Conduct or Certification Scheme, and the Council is not aware of any such Codes or Schemes in relation to CCTV.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The Council collects the data for the public's benefit through the prevention and detection of crime and to assist with the security of RMH for use by visitors and staff. The intended outcome is increased security of the building resulting in enhanced safety for staff and all users of the building.

The impact on individuals is minimal as the capture of the data is limited to that which is necessary to achieve the objectives. The cameras only record footage from entrances to the building and corridors/communal areas and do not have viewpoints into the rooms for hire.

Parish staff and all users of the building benefit by the processing of the CCTV data as it assists with the creation of a safe and secure environment through the prevention and detection of unlawful acts or antisocial behaviour.

The identified benefits are vital for the safety of staff and visitors to Roffey Millennium Hall, as well as the general security of the building and the prevention of any theft or damage.

If unable to process the data, the Parish Council would be less able to prevent and detect unlawful acts or antisocial behaviour which would result in a reduction to the safety of staff and visitors to the building.

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

CCTV is a well-established system that is often found in public places and buildings and is considered to be expected by the public. Therefore, considering the purposes and objectives of the CCTV system, i.e. the prevention and detection of crime and to assist with the security of RMH for use by visitors and staff, it is not considered necessary to consult with individuals.

Signage is located at the front of the building, visible from the exterior as well as internally to make everyone aware that CCTV is in operation, the reason for its operation and the Council's contact details.

The data is only accessible by the Clerk and Deputy Clerk and is password protected. All staff, including the Clerk and Deputy Clerk, have undergone training in Data Protection.

When necessary, the Council will liaise with the third party CCTV support provider should technical issues with the installation occur but the data itself is not shared with them.

Due to the basic set up of the system, there are no plans to consult experts, but this would be reviewed should the Council wish to significantly change the scope of the data collection by inclusion of other buildings or assets owned by the Council or as a result in changes in technology.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The Council relies on a legitimate interest for the processing CCTV data as the use of CCTV is widespread and common place, assists in making staff, visitors and hirers of the halls feel safe and can work with law enforcement agencies to prevent and detect crimes.

The lawful basis under UK GDPR is :-

> Article 6(1)(f) – Legitimate interests: prevention, detection or investigation of crimes, including the apprehension and prosecution of offenders

Alternatives to CCTV could include physical patrols but these would not offer the same level of deterrent 24 hours a day, would be unacceptably costly and would not offer the ability to provide evidence in the event of criminal activity. Therefore, alternatives have been rejected as not practicable.

Function Creep would be prevented through compliance with the Council's CCTV Policy and APD; restricting the use to the purpose of the activity i.e. prevention, detection or investigation of crimes, including the apprehension and prosecution of offenders; reviewing policies/documents/process when necessary; and through the appropriate training of staff.

Data quality will be ensured by using third party supported equipment under contract.

Data collection will be minimised by:-

- restricting to entrances, exits and main corridors
- visual only with no audio
- retained for 30 days and then automatically wiped unless it is downloaded in response to an incident, complaint or for disclosure
- Staff undergo appropriate training

Individuals will be made aware of the CCTV through the use of signage visible both inside and outside the building. The Council has an adopted CCTV Policy and Subject Access Request Policy and a Privacy Notice published on the Parish Council website.

The data is not transferred or shared outside of the Parish Council. All data is retained locally and backed up to physical server in the UK.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** Remote, possible or probable	**Severity of harm** Minimal, significant or severe	**Overall risk** Low, medium or high
System Breach or compromise resulting in unauthorised access to Data (compliance risk)	Remote	Minimal	Low
Data breach and publication of footage (compliance risk)	Remote	Minimal	Low
System failure (corporate risk)	Possible	Minimal	Low
ICO action in the event of non-compliance with GDPR	Remote	Minimal	Low

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk** Eliminated reduced accepted	**Residual risk** Low medium high	**Measure approved** Yes/no
System Compromise	• IT security including password protection • Only video data no audio recording • Camera location obvious and accessible	Accepted Accepted	Low Medium	Yes Yes
Data breach	• Staff Training • Restricted access to data from CCTV to senior staff members • Limited retention to 30 days with automatic wipe (unless downloaded in response to an incident, complaint or for disclosure)	Accepted	Low	Yes
System failure	• Contracted maintenance of equipment • Regular checks on recordings and deletion of 30 day plus data	Accepted	Medium	Yes
ICO action	• CCTV Policy and APD • Signage • Staff training • Privacy Notice published	Accepted	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:	S. Norman Clerk to the Council 02.04.26	Integrate actions back into project plan, with date and responsibility for completion
Residual risks	N/A	If accepting any residual high risk, consult the ICO before going

approved by:		ahead
DPO advice provided:	N/A	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: N/A		
DPO advice accepted or overruled by:	N/A	If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:	N/A	If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:	Clerk to the Council	The DPO should also review ongoing compliance with DPIA