Pound Hill Junior School

Data Protection Impact Assessment

Submitting controller details

Name of controller	Pound Hill Junior School
Subject/title of DPO	School Business Manager
Name of DPO	Rebecca Ngan

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.
We recognized the need for a DPIA as part of our commitment to data protection and compliance with the GDPR. Given the sensitive nature of a school environment, where the privacy of all users, especially children is paramount, we understand the importance of assessing and mitigating any potential risks associated with the introduction of CCTV systems. The DPIA process allows us to be transparent with our stakeholders, demonstrating that we value and protect their privacy. It also serves as a proactive measure to ensure that data protection principles are embedded into the CCTV project from its inception, aligning with best practices in data governance. For the purpose of the CCTV system, please refer to our CCTV policy.

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 CCTV system in our school is designed to collect visual data in the form of video footage. It does not record sound. This data is collected through strategically placed cameras in areas where monitoring has been identified as is necessary for security purposes. The source of the data is the live feed captured by these cameras, which may be viewed for purposes outlined in our CCTV policy.

Collection: Cameras are activated and recording 24 hours. They are positioned to avoid toilets and cubicles to respect the privacy of individuals. Cameras are recording during PE changing.

Usage: The footage is not used to monitor the premises in real-time and, if necessary, reviewed post-event to investigate reported incidents or security breaches. The entrance camera is monitored live to enable school office staff to identify and grant access to visitors promptly.

Storage: Data is stored on secure DVR with access restricted to authorised personnel only. We have implemented robust cybersecurity measures to protect this data from unauthorised access from a data breach. Recording of CCTV images is automatically suspended during times when pupils are regularly getting changed for PE and Games lessons. Staff must request that recording is suspended for ad-hoc events, additional or changes to PE and Games sessions, clubs and other events.

Deletion: Footage is retained for a period of 30 days unless it is required for an ongoing investigation or legal proceedings, after which it is securely deleted.

Sharing: We do not routinely share data with third parties. However, in specific instances such as a legal request from partner agencies such as the police, we may share footage in compliance with legal obligations.

High-Risk Processing: The types of processing identified as likely high risk involve the potential for misuse of data, unauthorised access, and the inadvertent capture of sensitive personal data. To mitigate these risks, we have strict policies and procedures in place, including regular audits, staff training, and technical safeguards such as encryption and access controls.

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 nature of the data collected by our school's CCTV system consists primarily of video recordings. These recordings capture the visual likeness of individuals within the school premises, which is considered personal data under data protection law. The system does not record audio, nor does it include any form of biometric processing or recognition software. The data does not fall under 'special category data' as defined by GDPR, which includes details about an individual's race, ethnic origin, politics, religion, trade union membership, genetics, biometrics, health, sex life, or sexual orientation. However, it may occasionally capture footage related to criminal offences if an incident occurs within the camera's field of view. We capture necessary footage for the safety and security of our students and staff which means that we will be collecting data continuously. The data will be used for the purposes of maintaining a secure environment, investigating incidents, and providing evidence if required during a police investigation. We do not record during times where there is an increased risk of intrusion such as getting changed for PE and Games or other events such as changing for performances. Footage will be stored securely on encrypted DVR with restricted access. We will retain the recordings for a period of 30 days, after which they will be automatically overwritten, unless retained for further investigation or legal proceedings. The number of individuals affected by the CCTV system includes all students, staff, and visitors to the school. We estimate this to encompass approximately 400 individuals daily. The geographical area covered by the CCTV system is confined to the school premises, which may include entry points, corridors, classrooms (where changing for PE and Games is NOT recorded), common areas, offices, small reading rooms and the perimeter. In summary, our CCTV system is designed to collect and use data in a manner that is compliant with data protection laws, proportionate to the risks we aim to address, and respectful of the privacy rights of individuals.

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 relationship between our school and the individuals captured on CCTV is primarily that of an educational institution to its students, staff, and visitors. As a junior school, we have a duty of care to ensure the safety and security of all individuals on our premises, particularly children and other vulnerable groups. *Individuals have limited control over the data collected by CCTV as it is a passive system. However, they are informed about the presence of CCTV through clear signage and our data protection policy, which outlines their rights under GDPR, including the right to access their data or request deletion in certain circumstances.* *The use of CCTV is a widely accepted practice in schools across the UK, and individuals generally expect such measures to be in place for security purposes. We have taken steps to ensure that our use of CCTV is in line with these expectations and does not extend beyond the common practices of similar institutions.* *We are sensitive to the context of the building in that the classrooms are regularly used for changing for PE as well as at other times during the academic year.* *Our school caters for children aged 7 to 11, who are considered a vulnerable group. Therefore, we have implemented stringent measures to ensure that the CCTV system is used responsibly, with footage accessed only by authorised personnel for specific, legitimate purposes.* *There have been no prior concerns raised regarding this type of data processing or security flaws in our system. We have conducted a thorough security assessment to ensure that the technology and practices we employ are robust and up-to-date.* *The CCTV technology we use is not novel; it is standard within the industry and reflects the current state of technology, including necessary encryption and access controls to safeguard the data.* *In light of public concern over privacy, we have considered the expectations of our community in our decision-making process to ensure that our practices align with ICO guidance and best practice.* *Lastly, our school is committed to adhering to any approved code of conduct or certification scheme related to data protection and surveillance once they are available. We continuously monitor developments in this area to ensure our practices remain compliant and reflect best practices in data governance.*

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?

Our primary goal with the implementation of CCTV within our school is to enhance the safety and security of our students, staff, and visitors. We aim to achieve a secure environment where educational activities can be conducted without the fear of disruption or harm.

Intended Effect on Individuals:

For Students: The presence of CCTV is intended to provide a sense of safety, deterring potential bullying, theft or vandalism, and ensuring a conducive learning atmosphere.

For Staff: It offers reassurance that incidents can be reviewed if necessary, providing support in disciplinary matters and protecting against false allegations.

For Parents: It gives confidence in the school's commitment to safeguarding their children and maintaining a secure environment.

Benefits of Processing:

Operational Efficiency: Quick resolution of disputes or incidents with clear evidence, reducing the time spent on investigations.

Preventative Measure: Acts as a deterrent against potential security threats or misbehaviour, contributing to a decrease in such incidents.

Legal Compliance: Ensures adherence to safety regulations and legal obligations to protect those on school premises.

Community Confidence: Builds trust within the school community, demonstrating transparency and accountability in our operations.

More broadly, the benefits extend to creating a culture of safety that permeates every aspect of school life. It contributes to the overall well-being of the school community and fosters an environment where education can thrive without undue concern for physical or emotional harm.

In summary, the CCTV system is not just a tool for surveillance but a means to support the educational mission of our school by promoting a safe and orderly environment.

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?

In the process of implementing the CCTV system, we recognise the importance of consulting with various stakeholders to ensure the project aligns with the needs and expectations of our school community.

Consultation Process:

Initial Phase: We will hold meetings with school leadership, including the headteacher and governors, to discuss the objectives and scope of the CCTV system.

Staff Engagement: Teachers and support staff will be invited to share their views through staff meetings and anonymous surveys.

Parental Input: Parents will be informed about any changes to the CCTV system via newsletters and parent-teacher meetings, where they can provide feedback.

Student Involvement: Older students will have the opportunity to express their opinions through student council discussions.

Data Processor Coordination: We will work closely with our data processors, who manage the CCTV footage, to ensure they understand the importance of data protection and security.

Expert Consultation: Information security experts will be consulted to assess the system's security measures and compliance with data protection laws.

Internal Involvement:

Data Protection Officer (DPO): Our DPO will be involved throughout the process to oversee compliance with GDPR and other data protection regulations.

Facilities Management: This team will provide insights into the practical aspects of camera placement and maintenance.

External Assistance:

CCTV System Provider: We will seek advice from our IT provider and CCTV consultants on best practices for installation and operation.

Legal Counsel: To ensure all legal aspects are covered, we will consult with legal experts from WSCC specialising in data protection law.

By engaging with these stakeholders, we aim to create a balanced and well-informed approach to the use of CCTV in our school, ensuring that the system serves its intended purpose without compromising the privacy and rights of individuals.

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?
Our lawful basis for processing personal data through CCTV is grounded in the legitimate interests of ensuring the safety and security of our students, staff, and visitors. This basis is in accordance with Article 6 of the GDPR, which allows for processing necessary for the purposes of the legitimate interests pursued by the school or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects. Achieving Our Purpose: The processing of CCTV footage is tailored to achieve our purpose of enhancing security. The system is designed to monitor only public areas where surveillance is necessary, and not private spaces or periods of increased sensitivity such as changing, ensuring that we respect the privacy of individuals. Alternative Measures: We have considered alternative measures, such as increased staffing and improved lighting, but have determined that these alone cannot provide the same level of continuous and effective monitoring that CCTV offers. Preventing Function Creep: To prevent function creep, we have clear policies in place that outline the specific purposes for which the CCTV system is used. Any expansion of these purposes will require a separate DPIA and approval process. Data Quality and Minimisation: We ensure data quality by maintaining our CCTV equipment regularly and ensuring that the footage is clear and usable. Data minimisation is achieved by retaining footage for only 30 days unless it is needed for an ongoing investigation. Information to Individuals: Individuals are informed about the CCTV system through clear signage, our data protection policy, CCTV Policy and privacy notices that are accessible on the school's website and upon request. Supporting Individual Rights: We support the rights of individuals by providing them with access to their data upon request, the ability to object to processing, and the right to be forgotten, in line with GDPR provisions. Processor Compliance: Our processors are contractually bound to comply with GDPR and our data protection standards. We conduct regular audits to ensure their adherence to these obligations.

Safeguarding International Transfers:

Although our data is not transferred internationally, should the need arise, we will implement standard contractual clauses, or rely on an adequacy decision, to ensure the protection of personal data.

This approach ensures that our use of CCTV is compliant with data protection laws, proportionate to our needs, and respectful of the rights of individuals.

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	Severity of harm	Overall risk
1. Privacy Intrusion: The most significant risk comes from the potential intrusion into individuals' privacy. This is particularly sensitive in areas where individuals have a higher expectation of privacy.	Possible	Significant	Medium
2. Data Breach: There is a risk of unauthorised access to the CCTV footage, either through cyberattacks or internal security failures.	Remote	Significant	Low
3. Misuse of Data: There is a potential risk that CCTV footage could be used for purposes other than those originally intended, known as 'function creep'.	Remote	Significant	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 (likelihood/risk level)	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Privacy intrusion (Low/medium)	1. Privacy Impact Filters: Where possible, employ privacy impact filters on cameras to obscure individuals' identities when not necessary for the intended purpose.	Reduced	Low	No
Privacy intrusion (medium/high)	2. Avoid live viewing of recordings for classrooms.	Reduced	Low	Yes
Privacy intrusion, data breach (medium/high)	3. Suspend recording of images during changing (and other sensitive events)	Reduced	Low	Yes
Privacy intrusion, Data breach, Misuse of Data (medium/medium)	4. Policy Review and Updates: Regularly review and update our CCTV policies to reflect changes in technology, legal requirements, and best practices.	Reduced	Low	Yes (yearly review)
Privacy intrusion (medium/medium)	5. Data Minimisation Techniques: Implement data minimisation techniques such as setting cameras to record at lower resolutions when high detail is not necessary.	Reduced	Low	No
Data breach, misuse of data (high/medium)	6. Enhanced Access Controls: Implement more stringent access controls to the CCTV footage, including multi-factor authentication and strict access logging.	Reduced	Low	Yes (limiting access to HT and DPO)
Data breach (low/high)	7. Advanced Encryption: Upgrade our data encryption methods to ensure that footage is protected both in transit and at rest.	Reduced	Medium	Yes

Data breach (low/high)	8. Regular Security Audits: Increase the frequency of security audits to ensure that all system vulnerabilities are identified and addressed promptly.	Reduced	Low	Yes (termly)
Data breach (low/high)	9. Incident Response Training: Provide specialised training for our staff on how to respond effectively to data breaches or security incidents.	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Steve Uwins/ Chair of Governors/ 6th September 2024	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Steve Uwins/ Chair of Governors/ 6th September 2024	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Rebecca Ngan/ School Business Manager/ 6th September 2024	DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice: Provided that the school implements the measures mentioned in step 6 and adheres to the CCTV policy, the use of CCTV should not pose an undue risk to the rights and freedoms of data subjects and can be carried out in compliance with data protection laws.		
DPO advice accepted or overruled by:	Steven Uwins/ Chair of Governors/ 6th September 2024	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 kept under review by:	The Governing Body, September 2025	The DPO should also review ongoing compliance with DPIA