School's CCTV Policy

Reviewed: September 2025

Review date: September 2028

DPIA for installation of surveillance camera system.

Name of School/Trust acting as the data controller:	**Dobcroft Junior School**
Name and Position of Individual(s) responsible for DPIA:	Nicola Sexton Amber Higgins
Name of DPO:	**Toby Wilson**
Date:	**July 2025**
Document prepared by:	**AH/TW**

Version	Date	Detail	Author
1.0	September 2025	DPIA for installation of surveillance camera system	Dobcroft Junior School

Introduction

The school intends to install a surveillance camera system on the premises with 14 external cameras and 5 internal cameras. There have been several incidents in these areas where reviewing footage would have been useful to aid the investigation of the incident.

The system records all of our staff, pupils and visitors whilst on the school site. The surveillance camera system assists in delivering the school's duty of care. It is an extension of the day-to-day physical supervision of all spaces within the school whilst pupils are present.

The system achieves its purpose by providing video data of any incident requiring investigation around the school site and act as a general deterrent. The surveillance camera system is a cost effective and efficient way to monitor site activity. It would not be practical or affordable to increase staffing levels to provide physical supervision of all the additional areas that require supervision. In addition, this could not be managed during the holiday periods and at night-time.

Screening questions

Will the project involve the collection of new information about individuals? If yes, please detail the information to be collected.
Yes, it will record images of individuals and their actions.

What is the lawful basis of the processing of this data?
Multiple lawful basis's for processing apply to the use of surveillance camera system;

- GDPR Article 6 (1)(c): Compliance with a legal obligation including the Safeguarding of children and staff, Management of Health and Safety at Work Regulations 1999, Health and Safety at Work Act 1974, Crime & Disorder Act 1998
- 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 school i.e. keeping our pupils safe whilst at school.
- GDPR Article 6 (1)(f): Where the school is processing CCTV footage for a legitimate reason other than performing its tasks as a public authority then this processing may be necessary for the purposes of our (or someone else's legitimate interests), except where overridden by the data subject's data protection rights and freedoms. The school and its visitors have a legitimate interest in being in a safe and secure environment while the legitimate interests of the school include protecting school buildings and property and the prevention and detection of crime and staff and visitor safety.

Will the project compel individuals to provide information about themselves? If yes, please detail the information to be provided.
The surveillance camera system recording compels individuals to provide their personal data, a surveillance camera system could be seen as privacy intrusive.

Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information? If yes, please detail which organisations will be provided with access.
Information will not be routinely disclosed to anyone outside the school staff. However, where necessary we will share data with:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- In the course of legal action/proceedings to relevant representatives such as solicitors.
- Persons recorded and whose images are retained where disclosure is required by virtue of Data Protection Legislation (DPA2018) and the Freedom of Information Act 2000.

Any data sharing to 3rd parties will be done following the latest guidance from ICO

Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? If yes, please describe the new purpose below.
Yes- it will be used for the reasons stated above.

Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition. If yes, please detail the new technology, below.
No. The system does not feature facial recognition or any other new technologies.

Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them? If yes, please describe the impact, below.
Yes, if evidence is obtained of wrong-doing, including criminal behaviour, this may lead to prosecution, civil claims, disciplinary procedures (staff or pupil) or exclusion (pupil).

Will the project require you to contact individuals in ways that they may find intrusive? If yes, please describe how the individuals will be contacted, below.
No

Note regarding Consultation
The school will consult with governors prior to any new installation.

<u>Step one: Identify the need for a DPIA</u>

What will the benefits be to the organisation, to individuals and to other parties?

Organisational benefits	Individual benefits	Other party benefits
● Protect the School buildings and School assets, both during and after School hours ● Enable a faster and more effective resolution to incidents. ● Safeguard students absent from lessons through visible checks about location during the school day and also during lunch; ● Reduce the incidence of vandalism, anti-social behaviour and site incursion; ● Assist senior staff in identifying persons who have or who are likely to have committed a breach of the school rules, including bullying and other anti-social behaviours.	Secure the health and safety of staff, parents, pupils and visitors. Greater parent and student confidence in school ability to maintain a safe and secure environment.	Assist in any criminal or safeguarding investigation

How many individuals are likely to be affected?
The whole school community, including staff, pupils and visitors.

If sensitive personal data is involved, have you established how this will be handled, accessed, retained and disposed of?
No special category data is directly processed, but footage may indicate special category data (i.e. disabilities, ethnicity, criminal activity, or other sensitive information may be recorded).

Is information quality good enough, how will data be verified & recorded accurately?
The system will be checked on a regular basis for image and capture quality. Authorised staff that regularly use the system and will report any issues with it.

Will training and instructions be given to appropriate staff to ensure compliance with policy and procedure?

Yes, authorised staff will be given training on the correct use of the system and handling any footage.

How will data subjects be able to access their rights in relation to the data?
Individuals visiting the site will be made aware of the surveillance camera system presence and scope of activity. They will know to expect data processing through a surveillance camera system via privacy notice and clear on-site signage.

It is reasonable to assume that most visitors are aware that the school uses a surveillance camera system. This is not a novel application of monitoring, as many schools use a surveillance camera system to promote health and safety and appropriate safeguarding measures.

This will promote transparency and the right to be informed. The right of access is detailed in the privacy notice on the school's website. Individuals may not necessarily have the right to restrict or rectify the data due to the nature of a surveillance camera system processing although this will be judged on a case by case basis. The right to erasure will be of limited application when the retention period is short. The right to erasure will be applicable where there is no lawful basis for retaining the data. Data portability is not applicable and there are no occasions where automated decision making is performed during this processing activity.

Step two: Describe the information flows

How is information collected?

The system is made up of a number of fixed cameras both inside and outside the building.

These are connected via network cables and footage is recorded on a specific server located within the school. The server is stored securely within the school with restricted access by staff. This is owned and managed by the school. Only authorised IT staff have physical and password access to the server.

Footage can be played back on certain PCs connected to the network.

Access is restricted to key members of staff and is not available to all staff.

Audio is not recorded.

The footage is held for 30 days and can be viewed until it is overwritten. If footage of an incident needs to be kept it can be exported to another secure location where it can be stored until it is no longer required.

The system is not accessible from external unless staff login remotely to their PCs via secure methods.

Where will the information be collected from?

See appendix A for locations of the new cameras and justification of their location

From whom/what is the information collected?

All users of the building including staff, students and visitors

What measures are in place to mitigate the risk of cyber-attacks which interrupt service or lead to the unauthorised disclosure of images and information?

The school has a Network firewall in place. Anti-virus, malware and ransomware protection are installed on both the server and client devices. Standard network security applies to access the school computers.

How is the information used?

Information is used to monitor pupil safety and security, protect property and prevent and detect crimes. Evidence is provided for investigation and enforcement. Individuals can request copies of CCTV data which contains their personal information. Disclosure of data is covered by internal processes which are fully compliant with relevant legislation and codes of practice.

How long is footage stored?

Data will be automatically overwritten or deleted every 30 days except where data has been exported for internal investigations. All retained data will be stored securely and permanently deleted as required by our data retention schedule. Recorded data kept securely on the School network in restricted folders. If a serious incident is recorded, it may be retained for DOB child +25 years, or 7 years for visitors/staff/parents.)

With which external agencies/bodies is the information/footage shared? (e.g. Supplier storage systems/Statutory prosecution agencies/Judicial system/Data subjects/Legal representatives/Local Authority/Other)

In common usage only internal authorised school/trust staff will access the footage

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- In the course of legal action/proceedings to relevant representatives such as solicitors.
- Data Subjects

How is the information disclosed where necessary? (e.g. Onsite visiting/copies of footage sent by mail/courier/etc/Offsite from remote server/Other)

- Onsite viewing where possible
- Secure transfer of digital files if necessary

Is there a written policy?

The school has a CCTV Code or Practice which is shared with all authorised users.

Are there auditing mechanisms?

The DPO and Office Manager regularly meet to discuss data protection issues and will address issues relating to CCTV where necessary.

Do operating staff receive appropriate training including legislation issues/monitoring, handling, disclosing, storage and deletion of information/incident procedures/limits on system uses/other (specify)?

Yes all authorised staff have relevant training on use of the system and data protection.

Step three: Identify the privacy and related risks

Privacy Issue	Risk Rating (see table at Appendix C)	Risk to Individuals	Compliance risk	Organisational risk
Inappropriate/unauthorised Disclosure of surveillance camera system Data for example by: *Hacking of systems * Inadequate passwords/security *undisclosed monitoring *use of system by unauthorised personnel * Incorrect configuration of new software	4	May disclose data which would embarrass or reveal private details that could identify child/parents/visitors	Data Protection Principle at risk- fair and lawful processing	Non-compliance with the DPA, GDPR or other legislation can lead to sanctions, fines and reputational damage. Problems which are only identified after the project has launched are more likely to require expensive and complicated fixes. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the school. Public distrust about how information is used can damage an organisation's reputation and lead to loss of confidence/trust. Data losses which damage individuals could lead to claims for compensation.
Poor or missing signage leads to individuals being captured by surveillance camera system without being aware of it	6	Individuals may behave in a way that they wouldn't if they knew surveillance camera system was in place	Data Protection Principle at risk- right to be informed	
Loss/accidental destruction of Data by school	4		Data Protection Principle at risk- secure storage of data	
Excessive collection of data by school exceeding purposes of system, invasion of privacy	4	High levels of information which is disproportionate to	Data Protection Principle at risk- adequate, relevant and not excessive	

• Location of cameras • Direction of cameras • Public highways • Washroom areas • Children's changing areas (hall and cloakrooms)		contract requirements.		
Retention of images/information for longer than necessary	4	May disclose data to a third party	Data Protection Principle at risk- not kept longer than necessary	
Inappropriate access by unauthorised staff	4	Data could be shared to wrong staff member	Data Protection Principle at risk- fair and lawful processing.	
Collection of special category data (as defined by DPA2018)	2	Sensitive data is inappropriately disclosed	Data Protection requirements relating to special category data- suggest school relies on “Vital Interest” but the collection must be proportionate to the aim perused and will depend on individual scenarios.	

Step four: Identify privacy solutions and sign off and record the DPIA outcomes

Risk	Solution(s)	Risk Rating after solution applied (see table at Appendix C)
All items identified in Step three above	Limit number of users of the surveillance camera system to authorised staff only and ensure access is logged.	2
	Carefully consider new locations of additional camera/s and what is being captured. Ensure cameras are not hidden or covert. Limit camera capturing the public highway.	2
	Carefully position new cameras so as not to capture inappropriate material such as pointing toward toilet cubicles or urinals - The school has enabled privacy masks in areas which may be contentious.	2
	Ensure configuration of new cameras and equipment is correct e.g audio functions are disabled.	2
	Ensure configuration of new software is secure and complex unique passwords are used	2
	Restrict or disable the use of remote access to the surveillance camera system or enforce two factor authentication on any device that has access	2
	Ensure signage is clearly displayed and privacy notices are amended so individuals are aware they are being captured on surveillance camera system. Check signage regularly for damage or unauthorised removal	2
	Ensure staff accounts and levels of access are kept up to date (e.g. when a staff member leaves or ceases to have the relevant responsibility their access is removed)	2
	Ensure staff follow Code of Practice guidance around the correct use of captured footage	2

	Staff training and supervision in correct usage of the software and regular reminders of their role in Data Protection compliance and safeguarding responsibilities	2
	Ensure captured data is deleted in accordance with the school Data Retention Policy	2
	Keep use of surveillance camera system under regular review to ensure it remains necessary, proportionate and effective in meeting stated purpose	2
	Test system regularly, install software and firmware updates to ensure system is reliable and secure. Replace faulty hardware quickly to ensure system is effective.	2
	Maintain an asset register for all hardware (including cameras) software and firmware, including any mitigation/comments on each camera location.	2

Risk Rating Decision

As a result of the privacy risks and mitigations it has been evaluated that the overall level of residual risk to privacy for the use of this software stands at Level X (see Appendix C). This is not a high risk and therefore we do/do not need to consult with the ICO.

Step five: Integrate the DPIA outcomes back into the project plan

Action To be Taken	Date of completion	Responsibility for
Review camera location and directions ensuring that coverage is appropriate	Sept 2025	A Higgins
Consult with SLT, DPO and Governors/Trustees. Consult with student groups, parent groups, staff groups	Sept. 2025	N Sexton
Approval of the final version of this DPIA by DPO	Sept 2025	N Sexton
Update information asset register and record of processing activities as necessary		A Higgins
Amend Privacy Notice(s) if necessary	Sept 2025	A Higgins
Amend relevant policies e.g. Information Security Policy, surveillance camera system/CCTV Policy, IT Policy and Acceptable User Agreement, Safeguarding and Child Protection Policy [any others relevant to individual school	Sept 2025	T Wilson
Install additional appropriate signage as required, replace signs that are damaged or not clearly readable	Oct 2025	A Higgins I Koszlinski
Establish regular review of this DPIA and the function of the surveillance camera system	Sept. 2025	A Higgins T Wilson - regular GDPR check ins
Ensure authorised staff are trained on appropriate use of system and data protection implications.	Sept 2025	A Higgins N Sexton S Doyle A Kirk P Harrison

Project Plan Approved by: Head Teacher

Date: October 2025

Appendix A: List of new camera locations (all fixed wall mounted camera)

Camera location	Sensitive location?	Main justification
Hall	No	Behaviour in the area, bullying incidents in toilet areas
Y3 Cloakroom	No	Behaviour in the area, bullying incidents in toilet areas
Y5 Cloakroom	No	Behaviour in the area, bullying incidents in toilet areas
Y4 Double Cloakroom	Yes (toilet entrance) - privacy mask applied	Behaviour in the area, bullying incidents in toilet areas
Y6 Cloakroom	No	Behaviour in the area, bullying incidents in toilet areas
Y4 Single Cloakroom	No	Behaviour in the area, bullying incidents in toilet areas
Marjorie's Garden X 2	No	Vandalism of school property and premises security
Back yard X 3	No	Vandalism of school property and premises security
Field X 4	No	Vandalism of school property and premises security
Front tyre park	No	Vandalism of school property and premises security
Front yard X 3	No	Vandalism of school property and premises security

Appendix B: Linking the DPIA to the Data Protection Principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Principle 1
Lawfulness, fairness and transparency of data processing
There must be lawful basis for processing the personal data as follows;
(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.

- Have you identified the purpose of the project and which lawful basis applies? Y

Is the processing of the data necessary in terms of GDPR? Y

How will you tell individuals about the use of their personal data?

Via privacy notice and by notices around school premises

Do you need to amend your privacy notices? N

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

n/a

If special categories of personal data have been identified have the requirements of GDPR been met? Y

As the School is subject to the Human Rights Act, you also will, where privacy risk are especially high, need to consider:

Will your actions interfere with the right to privacy under Article 8? Y

Have you identified the social need and aims of the project? Y

Are your actions a proportionate response to the social need? Y

Principle 2
Personal data shall be obtained only for one or more specified explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

Does your project plan cover all of the purposes for processing personal data? Y

Have you identified potential new purposes as the scope of the project expands? Y

Does your Privacy Notice cover all potential users? Y

Principle 3
Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used? Y

Which personal data could you not use, without compromising the needs of the project?

n/a

Principle 4
Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary? N

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

By regular checks of the system by authorised staff

Principle 5
Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.

What retention periods are suitable for the personal data you will be processing?

This will depend on the information gathered- see main document for full details

Are you procuring software that will allow you to delete information in line with your retention periods? Y

Principle 6
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Do any new systems provide protection against the security risks you have identified? Y

What training and instructions are necessary to ensure that staff know how to operate a new system securely?

All authorised staff receive training on the correct use of the system and the acceptable sharing of captured footage

Rights of Data Subjects and Privacy by Design

Will the systems you are putting in place allow you to respond to subject access requests more easily? Y

Will the system allow compliance with individual rights under GDPR, in particular the right to be informed, the right to rectification and Y the right to ensure (right to be forgotten).

If the project involves marketing, have you got a procedure for individuals to opt in to their information being used for that purpose?

n

Transferring data outside UK

Personal data shall not be transferred to a country or territory outside the UK unless that country of territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**.**

Will the project require you to transfer data outside of the UK? N

If you will be making transfers, how will you ensure that the data is adequately protected?

n/a

Code of practice for authorised operators

1. Dobcroft Junior School understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.
2. Dobcroft Junior School notifies all pupils, staff and visitors of the purpose for collecting surveillance data via privacy notices and clear signage.
3. Only authorised operators will have access to the system
4. In general staff will not live monitor cameras unless there is a clear justification for doing so such as a safeguarding concern. In some instances certain cameras such as gate cameras or entrance cameras may be live monitored by specific staff for short periods of time to check who is entering the premises and building.
5. All surveillance footage will be kept for 30 days to allow review subsequent to any reported incident.
6. Operators will only review footage with a clear purpose which must be recorded.
7. Where possible, reviewing of the footage should be done in the presence of **two or more** authorised operators. Footage must not be reviewed in an area where other unauthorised persons can observe.
8. Access to any footage must be logged with date, reason for access and the names of the observers (see next page).
9. Any footage taken offline will be stored securely and only on Dobcroft Junior School devices or systems.
10. Any footage shared with 3rd parties must be shared securely using encryption, password protection or other secure method.
11. Authorised operators will keep their account credentials secure at all times and will not share their account with anyone else.
12. Operators will report any technical issues quickly so any down time of the system is minimised

Authorised users:
Amber Higgins
Nicola Sexton
Sheree Doyle
Paul Harrison
Amy Kirk

Review Log

CCTV policy September 2025, awaiting ratification by the full board November 2025

Any authorised staff who requires to review footage needs to have a second authorised staff member with them and must complete this form detailing why the review is required.

Date	Reason for review	Staff name 2	Staff name 1