PINNER WOOD SCHOOL

SURVEILLANCE AND CCTY POLICY

Approval Authority	
Effective From:	November 2025
Date Ratified by GB:	
Next Review Date:	November 2026
Signed by Chair of GB:	

Contents:

 Statement of intent

At Pinner Wood Primary School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use surveillance cameras to monitor any instances of aggression or physical damage to our school and its members.

The purpose of this policy is to manage and regulate the use of the surveillance and CCTV systems at the school and ensure that:

- We comply with the UK Data Protection Legislation.
- The images that are captured are useable for the purposes we require them for.
- We reassure those persons whose images are being captured, that the images are being handled in accordance with data protection legislation.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing
- Taking action to prevent a crime
- Using images of individuals that could affect their privacy

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

1. Legal framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Regulation of Investigatory Powers Act 2000
- Protection of Freedoms Act 2012
- The UK General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- Freedom of Information Act 2000
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- School Standards and Framework Act 1998
- Children Act 1989

Children Act 2004 • Equality Act 2010 This policy operates in conjunction with the following statutory and non-statutory guidance:

- Home Office 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) 'Guide to the UK General Data Protection Regulation (UK GDPR)'
- ICO 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO 'CCTV& Video Surveillance'
- DfE 'Protection of biometric data of children in schools and colleges

This policy operates in conjunction with the following school policies:

- Photography and Images Policy

- Online Safety Policy
- Freedom of Information Policy
- School Security Policy
- Data Protection Policy

2. Definitions

For the purpose of this policy the following definitions are given for the below terms:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable.
- **Overt surveillance** – Surveillance which is clearly visible and signposted around the school and does not fall under the Regulation of Investigatory Powers Act 2000.
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance.

The school does not condone the use of covert surveillance when monitoring the school's staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

3. Roles and responsibilities

The role of the Data Protection Officer (DPO) includes:

- Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring consent is clear, positive and unambiguous. Pre-ticked boxes and answers inferred from silence are non-compliant with the UK GDPR.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.

- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school, their rights for the data to be destroyed and the measures implemented by the school to protect individuals' personal information.
- Preparing reports and management information on the school's level of risk related to data protection and processing performance.
- Reporting to the highest management level of the school, e.g. the governing board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's data protection impact assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the governing board.

The school, as the corporate body, is the data controller. The governing board therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The Headteacher deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks.

The role of the headteacher includes:

- Meeting with the DPO to decide where CCTV is needed to justify its means.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school is using surveillance fairly and lawfully.

- Communicating any changes to legislation with all members of staff.

4. Purpose and justification

The school will only use surveillance cameras for the safety and security of the school and its staff, pupils and visitors.

Surveillance will be used as a deterrent for violent behaviour and damage to the school.

The school will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility.

If the surveillance and CCTV systems fulfil their purpose and are no longer required, the school will deactivate them.

5. Data protection

Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA, or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA).
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
- Processed in a transparent manner, meaning that people are informed when their data is being captured.
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
    - Further processing for archiving data in the public interest
    - Scientific or historical research
    - Statistical purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up-to-date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The use of surveillance cameras and CCTV will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will be carried out prior to the installation of any surveillance, CCTV, or biometric system. A DPIA will:

- Describe the nature, scope, context, and purposes of the processing.
- Assess necessity, proportionality, and compliance measures.
- Identify and assess risks to individuals.
- Identify any additional measures to mitigate those risks.

If the DPIA reveals any potential security risks or other data protection issues, the school will ensure they have provisions in place to overcome these issues.

Where the school identifies a high risk to an individual's interests, and it cannot be overcome, the school will consult the ICO before they use CCTV, and the school will act on the ICO's advice.

The school will ensure that the installation of the surveillance and CCTV systems will always justify its means.

If the use of a surveillance and CCTV system is too privacy intrusive, the school will seek amendments.

Surveillance and CCTV systems will not be intrusive. Pupils, staff and visitors will be made aware of the following:

- Whenever they are being monitored by a surveillance camera system
- Who is undertaking the activity
- The purpose for which the associated information is being used

The use of any video conferencing technology will be fair and transparent. Any pupils and staff who are part of any video conference calls will be informed of its purpose and recording and publication of any video to an indefinite audience will be consented to and will not be used outside of the intended purpose.

6. Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.

The surveillance system is a closed digital system.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of the school.

7. Security

Access to the surveillance system, software and data will be strictly limited to authorised operators, and will be password protected, and where appropriate, will be encrypted.

In exceptional cases where large amounts of information need to be collected and retained, the school will consider using cloud storage. This will be secure and only accessible to authorised individuals.

The school's authorised CCTV system operators are:

- Miss Sarah Marriott Headteacher.
- Mr Carl Batson, Site Manager
- Mr Cindy Tong, Business Manager

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's authorisation forms will be completed and retained.

Surveillance and CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times.

The DPO and headteacher will decide when to record footage, e.g. a continuous loop outside the school grounds to deter intruders.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

The ability to produce copies of information will be limited to the appropriate staff.

Any unnecessary footage captured will be securely deleted from the school system.

Each system is visual therefore no audio recording takes place.

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

Visual display monitors are located in the Site Manager's Office and The Main Office.

8. Code of practice

The school understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, signs, letters and emails.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All surveillance footage will be kept for 30 days for security purposes; the headteacher and the data controller are responsible for keeping the records secure and allowing access.

The school has a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

The surveillance and CCTV system is owned by the school and images from the system are strictly controlled and monitored by authorised personnel only.

The school will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school's website. The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data.
- Be transparent and include a contact point which enables people to request information and submit complaints via the DPO.
- Have clear responsibility and accountability procedures for images and information collected, held and used.
- Have defined policies and procedures in place which are communicated throughout the school.
- Only keep images and information for as long as required.
- Restrict access to retained images and information with clear rules on who can gain access.

- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law.
- Be subject to stringent security measures to safeguard against unauthorised access.
- Be regularly reviewed and audited to ensure that policies and standards are maintained.
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
- Be accurate and well maintained to ensure information is up-to-date.

9. Access

Any individual recorded in any CCTV image is considered a data subject and therefore has the right to request access to those images.
These requests will be considered a Subject Access Request and should follow the school's Subject Access Request process by making a request via office@pinnerwood.co.uk

When such a request is made, the footage will be reviewed in accordance with the request.
If the footage contains only the data subject making the request, then the individual may be permitted to view the footage.
This will be strictly limited to the footage of the data subject making the request and the specific reason for the request.
If the footage contains images of other data subjects, then the school will consider whether.

- The request requires the disclosure of the images of data subjects other than the requester, and whether these additional data subjects can be anonymized in the footage.
- The other individuals in the footage have consented to the disclosure of the images or if their consent could be obtained.
- If not, then whether it is reasonable in the circumstances to disclose those images to the data subject making the request.

The School reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other data subjects or jeopardise an ongoing investigation.

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)

- Relevant legal representatives – such as lawyers and barristers, with the consent of the data subjects.

10. Complaints

We take any complaints about our collection and use of personal information very seriously.

If you think that our collection or use of personal information is unfair, misleading or inappropriate, or have any other concern about our data processing, please raise this with the school in the first instance via office@pinnerwood.co.uk

This complaint may be assessed by our independent Data Protection Officer,

If you are unhappy with the school's final response you can refer the matter to the Information Commissioner's Office:

- Report a concern online at https://ico.org.uk/concerns/
- Call 0303 123 1113

11. Monitoring and review

This policy will be monitored and reviewed on an annual basis by the DPO and the headteacher.

The headteacher will be responsible for monitoring any changes to legislation that may affect this policy, and make the appropriate changes accordingly.

The headteacher will communicate changes to this policy to all members of staff.

The scheduled review date for this policy is **November 2026**.