Reviewed: October 2024
Next Review Date: October 2026

Signed by:

Claire Jones	Headteacher	Date: October 2024
Andy Oddy	Chair of Governors	Date: October 2024

Euxton Primrose Hill School Surveillance and CCTV Policy

Table of Contents

Surveillance and CCTV Policy

Introduction

At Euxton Primrose Hill 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.

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

- The school complies with the UK General Data Protection Regulation
- 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.

Purpose of this policy

The school complies with the Home Office's Surveillance Camera Code of Practice 2021 and ICO guidance regarding CCTV systems.

The surveillance system will be used to:

- Maintain a safe environment
- Protect school buildings and assets
- 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.

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

If the surveillance system fulfils its purpose and are no longer required, it will be deactivate.

The school will ensure that CCTV warning signs are clearly and prominently placed at all external entrances and where CCTV is used. Signs will contain details of the purpose for using CCTV.

Legal Framework

This policy has due regard to legislation including, but not limited to, the following:

- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The General Data Protection Regulation
- The 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

This policy has been created with regard to the following statutory and non-statutory guidance:

- Home Office (2021) 'Surveillance Camera Code of Practice'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'
- ICO (2022) 'Guidance on Video Surveillance'

Roles and Responsibilities

It is the responsibility of all members of the school to comply with the CCTV policy and any related procedures in accordance with ICO recommendations.

Data Protection Officer

The role of the data protection officer (DPO) includes:

- Dealing with freedom of information requests and subject access requests (SAR) 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 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 school board.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Presenting reports regarding data processing at the school to senior leaders and the governing board.

Data Controller

Euxton Primrose Hill Primary School 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 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.

Headteacher

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.

Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the surveillance code of conduct:

- 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 – any use of surveillance for which authority 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 staff, pupils, and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

Any overt surveillance footage will be clearly signposted around the premises.

Data Protection and Data Protection Impact Assessments

Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA, or from advice from the DPO.
- 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, CCTV, and biometric systems 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.

Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR).

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 will act on the ICO's advice.

Surveillance and CCTV systems will not be intrusive. If the use of a surveillance and CCTV system is too intrusive, the school will seek amendments. Pupils, staff and visitors will be made aware of the following via notices on the premises:

- 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

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

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 use cloud-based storage. This will be secure and only accessible to authorised individuals.

The school's authorised CCTV system operators are:

- Joanne Vost, SBM
- Angela Thompson, Office Manager
- Lisa Griffiths, Office Administrator

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 regularly tested for security flaws to ensure that they are being properly maintained at all times.
The DPO and Principal will decide when to record footage, e.g. a continuous loop outside the premises 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 system.

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 main office and the SBM's office.

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

Surveillance footage will be kept for six months for security purposes.

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

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 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, the DPO, through which people can access information and submit complaints.
- 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.

Siting the cameras

Cameras will be sited to only capture images relevant to the purposes for which they are installed; care will be taken to ensure that reasonable privacy expectations are not violated.

CCTV cameras will be located at strategic points on external points of the premises to cover the external area and access points.

Access to CCTV images

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed. All data containing images belong to, and remain the property of, the school
Individuals have the right to submit an SAR to gain access to their personal data in order to verify the lawfulness of the processing.

The school will verify the identity of the person making the request before any information is supplied.

A copy of the information will be supplied to the individual free of charge; however, the school may impose a 'reasonable fee' to comply with requests for further copies of the same information.
Where an SAR has been made electronically, the information will be provided in a commonly used electronic format.

Requests by persons outside the school for viewing or copying disks, or obtaining digital recordings, will be assessed by the DPO on a case-by-case basis with close regard to data protection and freedom of information legislation.

Where a request is manifestly unfounded, excessive or repetitive, a reasonable fee will be charged. All fees will be based on the administrative cost of providing the information.

All requests will be responded to without delay and at the latest, within one month of receipt.
In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, the school holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.
In the event that a large quantity of information is being processed about an individual, the school will ask the individual to specify the information the request is in relation to.

Where data requests contain the personal data of a separate individual, the rights and freedoms of others will be protected by asking for their consent or removing specific footage where appropriate.

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
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Complaints

Complaints and enquiries about the operation of CCTV within the school should be directed to the DPO in the first instance. Data subjects also have the right to complain to the ICO: https://ico.org.uk/make-a-complaint/

Monitoring and Review

The primary purpose of this policy is to ensure processing of CCTV data is done so in accordance with the legal obligations of the school under the General Data Protection Regulation (GDPR).

Monitoring of systems in place will be undertaken through internal quality assurance processes by the Data protection Officer (DPO). This policy is reviewed every two years by the DPO.

Contact

Contact the Data Protection Officer by:

Email: bursar@primrosehill-euxton.lancs.sch.uk

Phone: 01257 276688 or

Post: Euxton Primrose Hill Primary School, Primrose Hill Road, Euxton, PR7 6BA

Version Control

Named Owner:	Mrs Joanne Vost – Data Protection Officer
Version Number:	1.00
Date Of Creation:	October 2024
Last Review:	October 2024
Next Scheduled Review:	October 2026
Overview of Amendments to this Version:	New policy