Latymer All Saints
C of E Primary School

Latymer All Saints C of E Primary School
CCTV Policy

1. PURPOSE

The Purpose of this policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Latymer All Saints CofE Primary School, hereafter referred to as 'the School'.

CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its associated equipment as well as creating a mindfulness among the occupants, at any one time, that a surveillance security system is in operation within and/or in the external environs of the premises during both the daylight and night hours each day. CCTV surveillance at the School is intended for the purposes of:

- protecting the School buildings and assets;
- promoting the health and safety of staff, pupils and visitors as well as for monitoring student behaviour;
- preventing bullying;
- reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- supporting the police in a bid to deter and detect crime;
- assisting in identifying, apprehending and prosecuting offenders; and
- ensuring that the School rules are respected so that the School can be properly managed.

The system does not have sound recording capability.

The CCTV system is owned and operated by the School, the deployment of which is determined by the School's leadership team.

the School is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).

All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are made aware of their responsibilities in following the CCTV Code of Practice. All employees are aware of the restrictions in relation to access to, and disclosure of recorded images.

2. SCOPE

This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The Academy complies with the Surveillance Commissioner's CCTV Code of Practice to ensure it is used responsibly and safeguards both trust and confidence in its use.

CCTV warning signs will be clearly and prominently placed at the main external entrance to the Academy. Signs will contain details of the purpose for using CCTV (see Appendix A).

The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, but it is not guaranteed that the system will cover or detect every single incident taking place in the areas of coverage.

CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the School, including Equality & Diversity Policy, Codes of Practice for dealing with complaints of Bullying & Harassment and Sexual Harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.

This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g. race, gender, sexual orientation, national origin, disability etc.

Video monitoring of public areas for security purposes within Academy premises is limited to uses that do not violate the individual's reasonable expectation to privacy.

Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the School or a student attending the School.

All CCTV systems and associated equipment will be required to be compliant with this policy following its adoption by the School. Recognisable images captured by CCTV systems are 'personal data'. They are therefore subject to the provisions of the General Data Protection Regulation and Data Protection Act 2018

3. LOCATION OF CAMERAS

The cameras are sited so that they only capture images relevant to the purposes for which they have been installed (as described above), and care will be taken to ensure that reasonable privacy expectations are not violated. the School will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation.

the School will make every effort to position the cameras so that their coverage is restricted to the School premises, which includes both indoor and outdoor areas.

CCTV will not be used in classrooms but in limited areas within the School that have been identified by staff and pupils as not being easily monitored.

CCTV Video Monitoring and Recording of Public Areas may include the following:

- Protection of buildings and property: The building's perimeter, entrances and exits, lobbies and corridors, special storage areas, cashier locations, receiving areas for goods/services
- Protection of staff and pupil's person and property: where an incident occurs which involves these matters, information may be shared with those involved to ensure the maintenance of safety and that matters such as theft and damage can be investigated
- Monitoring of Access Control Systems: Monitor and record restricted access areas at entrances to buildings and other areas
- Verification of Security Alarms: Intrusion alarms, exit door controls, external alarms
- Video Patrol of Public Areas: Parking areas, Main entrance/exit gates, Traffic Control
- Criminal Investigations (carried out by the police): Robbery, burglary and theft surveillance

5. STORAGE AND RETENTION OF CCTV IMAGES

Recorded data will not be retained for longer than 30 days except where the image identifies an issue and is retained specifically in the context of an investigation/prosecution of that issue.

Where data is retained for longer than 30 days an electronic file held on a secure central server where specific CCTV image/recordings are retained will be kept. The Data Protection Act and GDPR does not prescribe any specific minimum or maximum retention periods that apply to all systems or footage. Therefore, retention will reflect the School's purposes for recording information, and how long it is needed to achieve this purpose.

the School will store data securely at all times.

6**. ACCESS TO CCTV IMAGES**

Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available. Supervising the access and maintenance of the CCTV System is the responsibility of the Head of each school. The Head may delegate the administration of the CCTV System to another staff member. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis. Recording may be provided for investigation purposes and to pursue civil claims at the discretion of the Head.

7. SUBJECT ACCESS REQUESTS (SAR)

Individuals have the right to request CCTV footage relating to themselves under the Data Protection Act and the GDPR.

All requests should be made in writing to the Data Protection Officer who can be contacted by email to XXXXX. Individuals submitting requests for access will be asked to provide sufficient information to enable footage relating to them to be identified. For example: time, date and location.

The School will respond to requests within one calendar month of receipt.

The School reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation. We will use redaction (blurring etc.) in situations where the rights of others can be protected in this manner.

8. ACCESS AND DISCLOSURE OF IMAGES TO THIRD PARTIES

There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police, service providers to the School where these would reasonably need access to the data (e.g. investigators) and where required for the purposes noted above.

If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first instance and appropriate legal advice may be required.

Requests for images should be made in writing to the Data Protection Officer.

The data may be used within the School's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

9. RESPONSIBILITIES

The Head of each school will:

- Ensure that the use of CCTV systems is implemented in accordance with this policy.
- Oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the School.
- Ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
- Ensure that the CCTV monitoring is consistent with the highest standards and protections.
- Review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintain a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensure that monitoring recordings are not duplicated for release.
- Ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Give consideration to both students and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment.

- Ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the School and be mindful that no such infringement is likely to take place.
- Ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing and comply with the principle of "Reasonable Expectation of Privacy"
- Ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- Ensure that images recorded are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation, court proceedings (criminal or civil), a data protection request, or other bona fide use as approved by the Head of School.
- Ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas.

10. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN

CCTV has the potential to be privacy intrusive. the School will perform a Data Protection Impact Assessment when installing or moving CCTV cameras to consider the privacy issues involved with using new surveillance systems to ensure that the use is necessary and proportionate and address a pressing need identified.

11. COMPLIANCE WITH CODE

It is a requirement that all CCTV systems comply with code issued by the Surveillance Commissioner. This includes 12 principles; we document how we comply below.

Principle 1 Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.

The specific purposes are given in Objectives above. There is a pressing need for the School to ensure the safety of its staff pupils and visitors, and to protect its assets.

Principle 2 The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.

This has been carefully considered. Fixed cameras record continuously within their scope and public areas are excluded from scope. Mobile cameras are not used.

Cameras are not placed in enclosed areas where there is an expectation of privacy.

Principle 3 There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints.

This is provided by this policy.

Principle 4 There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.

The Head of School is responsible and accountable for all activities

Principle 5 Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.

These are provided by this policy

Principle 6 No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.

Recordings made by detection are deleted after 7 days unless action is taken to preserve them. This is only done where the recordings are required for one of the objectives noted above.

Principle 7 Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.

Only the roles noted above can access images except where required by law enforcement. The roles noted above will manage the viewing of images in normal use to meet the objectives above. Viewing of images by persons involved in incidents will be granted where necessary for the objectives.

Principle 8 Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.

These have been considered. As a technical standard, we have a minimum image size of 1080p to ensure sufficient clarity.

Principle 9 Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use.

Images are stored on the servers at the school. These are appropriately secured.

Principle 10 There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.

This policy is reviewed annually, the review date is at the end. No reporting is considered necessary by the governors except for logging of details of individual accesses for the purposes.

Principle 11 When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.

This principle is supported by this document.

Principle 12 Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.

No reference databases are used.

12. POLICY REVIEW

The Data Protection Officer is responsible for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

APPENDIX A

CCTV SIGNAGE

It is a requirement of the Data Protection Act to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. the School is to ensure that this requirement is fulfilled. The CCTV sign should include the following:

- That the area is covered by CCTV
- The name of the School.
- The contact telephone number or address for enquiries.