

CCTV Policy.



Version 2

Name of Policy writer Gill Smith

Last Updated December 2025

Review Date

Approved

ICO registration number Z6538316

Approved by:

Signature:

Position:

Chair of Govs.

Last reviewed on: N/A

Next review due by: February 2029

Amendments from previous version. New policy adopted Feb 26

Contents:

- A. Introduction
- B. Purpose
- C. Scope
- D. Location of cameras
- E. Storage and Retention of CCTV Images
- F. Access to CCTV Images
- G. Subject Access Requests
- H. Access and Disclosure of Images to Third Parties
- I. Responsibilities
- J. Breaches including security breaches
- K. Data Protection Impact Assessments and Privacy by Design
- L. Policy Review
- M. Appendix A – Plan of the location of cameras

A. INTRODUCTION

1. This policy is intended to clearly set out the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) which are relevant to Markland Hill School use of CCTV and video surveillance.
2. Markland Hill School has identified the most appropriate lawful basis for processing CCTV data under Article 6 UK GDPR and this is recorded on the Record of Processing Activities.
3. This policy applies to all our workforce including employees, trustees, governors, consultants, self-employed contractors, casual workers, agency workers and volunteers. It also applies to anyone visiting our premises.
4. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

B. PURPOSE

1. The Purpose of this policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Markland Hill School, which shall be hereafter referred to as "School". CCTV systems are installed externally on the premises for the purpose of enhancing security of the building as well as creating mindfulness among the occupants, at any one time, that a surveillance security system is in operation in the external environs of the premises during both the daylight and night hours each day.
2. CCTV surveillance on the premises and grounds is intended for the purposes of:
 - a. For the personal safety of staff, pupils, visitors and other members of the public and to act as a deterrent against crime
 - b. protecting the school buildings and school assets from damage, disruption, vandalism and other crime, both during and after school hours;
 - c. reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
 - d. supporting the police in a bid to deter and detect crime;
 - e. assisting in identifying, apprehending and prosecuting offenders; and
 - f. ensuring that the school rules are respected so that the school can be properly managed
 - g. to assist in day-to-day management of the School including ensuring the health and safety of staff, pupils and others
 - h. to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance procedures
 - i. to assist in the defence of any civil litigation, including employment tribunal proceedings
 - j. to assist in the effective resolution of complaints which arise
 - k. this list is not exhaustive, and other purposes may be or become relevant.
3. The CCTV system is owned and operated by the school, the deployment of which is determined by the school's leadership team.
4. The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and members of the school community.
5. The School's CCTV is registered with the Information Commissioner under the terms of the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) 2016/679.
6. All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images.
7. All operators are made aware of their responsibilities.
8. All employees are aware of the restrictions in relation to access to, and disclosure of recorded images.

C. SCOPE

1. This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. The school complies with the Information Commissioner
2. CCTV warning signs will be clearly and prominently placed at the main external entrance to the school. Signs will contain details of the purpose for using CCTV. In areas where CCTV is used, the school will ensure that there are prominent signs placed within the controlled area.
3. The planning and design have endeavoured to ensuring 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.
4. CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the school.
5. 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.
6. Video monitoring of public areas for security purposes within School premises is limited to uses that do not violate the individual's reasonable expectation to privacy.
 - Cameras with an audio recording function are not use in our school.
7. School does not use covert recording
8. 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.
9. 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.

D. LOCATION OF CAMERAS

1. 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 ensuring that reasonable privacy expectations are not violated. The school will ensure that the location of equipment is carefully considered to ensuring that the images captured comply with the legislation.
2. The school will make every effort to position the cameras so that their coverage is restricted to the school premises.
3. Members of staff will have access to details of where CCTV cameras are situated.
4. A plan of the location of the cameras should be appended to this policy (Appendix A)

E. STORAGE AND RETENTION OF CCTV IMAGES

1. 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.
2. 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 (G drive/GDPR/CCTV). The Data Protection Act and GDPR do 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.
3. The school will store data securely at all times.

F. ACCESS TO CCTV IMAGES

1. Access to recorded images will be restricted to the staff authorised to view them and will not be made widely available.
2. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member.
3. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.

G. SUBJECT ACCESS REQUESTS (SAR)

1. Individuals have the right to request CCTV footage relating to themselves under the Data Protection Act and the GDPR.
2. All requests should be made in writing to the Data Protection Officer who can be contacted by email to gill@mindography.co.uk. 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, location and if necessary, information identifying the individual.
3. We will respond to requests within 30 days of receiving the request but if a request is received outside of the school term this may not be possible. Applicants may view the CCTV footage if available and copies may be made available if they do not compromise the rights of others.
4. We reserve the right to obscure images of third parties when disclosing CCTV data as part of a Subject Access Request, where we consider it necessary to do so. Where the circumstances of an incident mean that it is not possible to effectively obscure images of third parties, we reserve the right to refuse the request on the basis that it would reveal the identities of third parties.
5. We reserve the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

H. ACCESS AND DISCLOSURE OF IMAGES TO THIRD PARTIES

1. There will be no disclosure of recorded data to third parties other than authorised personnel such as the Police and service providers to the school where there would be reasonable need access to the data (e.g. investigators).
2. 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.
3. Requests for images should be made in writing to the Data Protection Officer.
4. A record of disclosures of CCTV footage will be maintained.
5. 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.
6. No images from CCTV will ever be posted online or disclosed to the media.

I. RESPONSIBILITIES

1. The Headteacher responsibilities include:
 - Ensuring that the use of CCTV systems is implemented in accordance with this policy.
 - Overseeing and co-ordinate the use of CCTV monitoring for safety and security purposes within the school.
 - Ensuring that all existing CCTV monitoring systems will be evaluated for compliance with this policy.
 - Ensuring that the CCTV monitoring is consistent with the highest standards and protections.

- Reviewing camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy.
- Maintaining a record of access (e.g. an access log) to or the release of tapes or any material recorded or stored in the system.
- Ensuring that monitoring recorded tapes are not duplicated for release.
- Ensuring that the perimeter of view from fixed location cameras conforms to this policy both internally and externally.
- Giving 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.
- Ensuring 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.
- Ensuring 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”.
- Ensuring that monitoring tapes are stored in a secure place with access by authorised personnel only.
- Ensuring that images recorded on tapes/DVDs/digital recordings are stored for a period not longer than 30 days and are then erased unless required as part of a criminal investigation or court proceedings (criminal or civil) or other bona fide use as approved by the Headteacher/Head of School.
- Ensuring that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy.
- Ensuring that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics.
- Ensuring that camera control is not infringing an individual’s reasonable expectation of privacy in public areas.

2. The Data Protection Officer’s responsibilities include:

- 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 in schools 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.
- Preparing reports and management information on the school’s level of risk related the use of CCTV through termly audits.
- Reporting to the highest management level of the school, e.g. the governing board/trustees.
- Monitoring the performance of the School’s Data Processing Impact Assessment (DPIAs) in relation to the use of CCTV.

J. BREACHES INCLUDING SECURITY BREACHES

1. Any breach of the Code of Practice by school staff will be initially investigated by the Headteacher in order for them to take the appropriate disciplinary action.
2. Any serious breach of the Code of Practice will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach

K. DATA PROTECTION IMPACT ASSESSMENTS AND PRIVACY BY DESIGN

1. 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.

L. POLICY REVIEW

1. The Head Teacher is responsible for monitoring and reviewing this policy. This policy will be reviewed every 3 years.
2. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.