



Closed Circuit Television Policy

Author: Matt Stedman

Date: March 2022

Revised: March 2022

Statement of Intent

At Mayfield 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 data protection legislation, including the Data Protection Act 1998 and the General Data Protection Regulation (GDPR);
- 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

1. Legal framework

This policy has due regard to legislation and statutory guidance, including GDPR legislation.

This policy operates in conjunction with all school policies and procedures.

2. Definitions

For the purpose of this policy a set of definitions will be outlined, in accordance with the 2013 Home Office 'The Surveillance Camera Code of Practice' surveillance code of conduct:

- Surveillance – monitoring the movements and behaviour of individuals;

All surveillance cameras will be clearly visible around the school site.

3. Roles and responsibilities

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 and 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 (a maximum of 30 days);
- 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, the governing body;
- 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 body.

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

The Director of Business Operations 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 health, 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 toilet cubicles or any changing facility.

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

5. The data protection principles

Data collected from surveillance and CCTV will be:

- Processed lawfully, fairly and in a transparent manner in relation to individuals;
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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 are inaccurate, having regard to the purposes for which they are processed, are 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 are processed; personal data may be stored for longer periods, insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;
- 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.

6. Objectives

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.

The surveillance systems will be in the following locations:

Camera	Note(s)	Interior/Exterior	Retention Period
Central Courtyard Area		Exterior	
East Side External North		Exterior	
East Side External South		Exterior	
Main Entrance External		Exterior	
North East Stairs External		Exterior	
South East Stairs External		Exterior	
South West Stairs External		Exterior	
Sports Hall NE Area External		Exterior	
Sports Hall NW Corner External		Exterior	
Sports Hall External North Gate		Exterior	
Lift		Interior	
Year R – 3 Entrance	Ground floor	Interior	
Year R – 3 Rear Lobby	Ground floor	Interior	
Year 2 Corridor	Ground floor	Interior	
Year 6 Corridor	Ground floor	Interior	
Year 4 – 6 Entrance	Ground floor	Interior	
Year 4 -6 Rear Lobby	Ground floor	Interior	

Studio 1	Ground floor	Interior	
Studio 2	Ground floor	Interior	
Sports Hall Toilet Corridor	Ground floor	Interior	
Sports Hall 1	Ground floor	Interior	
Sports Hall 2	Ground floor	Interior	
Sports Hall 3	Ground floor	Interior	
Reception	Ground floor	Interior	
Main Hall 1	Ground floor	Interior	
Main Hall 2	Ground floor	Interior	
Main Hall 3	Ground floor	Interior	
Servery Corridor	Ground floor	Interior	
Music Corridor	Ground floor	Interior	
Kitchen	Ground floor	Interior	
Ground Floor Servery	Ground floor	Interior	
Pupil Services	Ground floor	Interior	
Dining Area Grab and Go	Ground floor	Interior	
Dining Area	Ground floor	Interior	
Dining Area Toilets	Ground floor	Interior	
Sports Hall Entrance	First floor	Interior	
The Cranny	First floor	Interior	
First Floor West towards the Cranny	First floor	Interior	
The Wilkie Library	First floor	Interior	
Sports Hall 1 st Floor Toilets	First floor	Interior	
First Floor Walkway	First floor	Interior	
First Floor SW Stairs	First floor	Interior	
First Floor SE Stairs	First floor	Interior	
First Floor NW Stairs	First floor	Interior	
First Floor Sports Hall Stairs	First floor	Interior	
First Floor Reflection Corridor	First floor	Interior	
Café Tranquillo	First floor	Interior	
First Floor Central Toilets	First floor	Interior	
First Floor East Corridor North	First floor	Interior	
First Floor East Corridor South	First floor	Interior	
Second Floor NE Toilets	Second floor	Interior	
Second Floor Central Toilets	Second floor	Interior	
Second Floor Central Corridor	Second floor	Interior	
Second Floor Lift Lobby	Second floor	Interior	
Second Floor East Corridor	Second floor	Interior	
Second Floor Hollow Corridor	Second floor	Interior	
Second Floor Reprographics Corridor	Second floor	Interior	
STEAM Prep Room	Second floor	Interior	
Second Floor SW Stairs	Second floor	Interior	
Second Floor SE Stairs/ Walkway	Second floor	Interior	
Sports Hall 2 nd Floor Stairs	Second floor	Interior	
Second Floor NE Stairs	Second floor	Interior	
Second Floor Sports Hall Stairs	Second floor	Interior	

7. Protocols

The surveillance system is a closed system which does not record audio.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice.

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 trained on individuals 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.

8. Security

Access to the surveillance system, software and data will be strictly limited to authorised operators.

The school's authorised CCTV system operators are:

- The Headteacher/Head of Seniors/Head of Primary;
- The Director of Business Operations;
- The Facilities Managers (deferred to a member of the site team when necessary – for example in the absence of the Facilities Managers);
- The Network Manager
- The Data Manager (deferred to the network technician when necessary – for example in the absence of the Network Manager);
- Verkada – the provider of the CCTV equipment.

Unauthorised access of the CCTV system will result in an investigation by the Director of Business Operations. Those found to access the CCTV without authorisation from/in the company of the operators above will be subject to disciplinary action.

The main control facility is accessed through a secure website that is password protected. Access to this website is controlled by the Data Manager. The CCTV system can be accessed remotely at any time through a secure internet connection.

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

Surveillance and CCTV systems will not be intrusive.

The DPO and Headteacher(s) will decide when to archive footage, e.g. a specific incident or violent behaviour or vandalism. Any unnecessary footage captured will be securely deleted from the school system.

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

9. Privacy by design

The use of surveillance cameras and CCTV will be critically analysed using a DIPA (data protection impact assessment). A DPIA will be reviewed prior to the installation of any additional surveillance and CCTV system equipment.

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.

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 alternative provision.

10. 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 signs in the school grounds where cameras are based.

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 up to 30 days for security purposes; the Headteacher and the data controller are responsible for keeping the system 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 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.

11. Access

Under the GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

Individuals have the right to submit a Subject Access Request (SAR) to gain access to their personal data in order to verify the lawfulness of the processing. Details of the school's response to a SAR are detailed in the Subject Access Request Policy.

Requests by persons outside the school for viewing images, or obtaining digital recordings, will be assessed by the Headteacher, who will consult 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 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.

It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure that the rights of individuals are preserved, but also to ensure that the chain of evidence remains intact, should the images be required for evidential purposes.

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.

Requests for access or disclosure will be recorded and the Headteacher will make the final decision as to whether recorded images may be released to persons other than the police.

12. Monitoring and review

This policy will be monitored and reviewed on a biennial basis, or in light of any changes to relevant legislation by the DPO and the Headteacher.

The Headteacher and the Director of Business Operations 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.