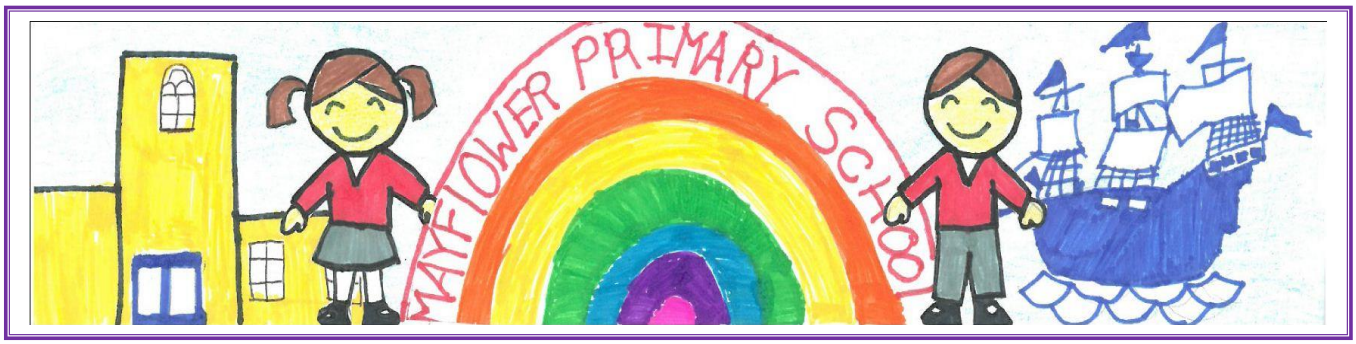
MAYFLOWER PRIMARY SCHOOL



CCTV POLICY
2020-2021

Mayflower Primary School operates one CCTV camera at the front of the school, linked to the buzz-entry system. It allows office staff to make an immediate determination in respect of who is trying to gain access to the school. In the event of a hostile entity, access can be denied, and help sought. Our CCTV Policy seeks to ensure that operation is in compliance with the law relating to Data Protection (currently the General Data Protection Regulations), and also the Data Protection Act (2018).

Policy Date:	March 2021		**Version:** 1		
Policy Review Date:	March 2023		Head Teacher: Luke Whitney		Insert Date
Ratified by Governing Body:					
Mrs. Y. Nana (Chair of Governors)			Insert Signature	24.03.21	

At Mayflower Primary School, we take our responsibility towards the safety of staff, visitors and pupils very seriously. To that end, we use a single surveillance camera to monitor the main entrance to the school building.

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

- We comply with data protection legislation, including the Data Protection Act 2018 and the General Data Protection Regulation (UK-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.

Legal framework

This policy has due regard to legislation and statutory guidance, 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 (UK-GDPR)
- The Data Protection Act 2018
- 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
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010

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

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- Information Commissioner's Office (ICO) (2017) 'Overview of the General Data Protection Regulation (UK-GDPR)'
- ICO (2017) 'Preparing for the General Data Protection Regulation (UK-GDPR) 12 steps to take now'
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and personal information'

This policy operates in conjunction with the following school policies:

- Photography and Videos at School Policy
- E-Safety Policy
- Freedom of Information Policy
- Data Protection Policy
- Privacy Notice

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. For the purpose of this policy both video and audio (limited to the area at the main entrance to the school) 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.
- Mayflower Primary 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.
- Any overt surveillance will be clearly signposted around the school, embracing the main entrance only

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. 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 Body.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school's Privacy Impact Assessment (PIA); and, under the UK-GDPR, the Data Protection Impact Assessment (DPIA); and providing advice where requested.
- Presenting reports regarding data processing at the school to senior leaders and the Governing Body.

Mayflower Primary School, as the corporate body, is the Data Controller. The Governing Body therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The School Business Manager deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy, will act as the main point of contact in relation to surveillance and CCTV footage.

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 Head Teacher 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 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.

Purpose and justification

The school will only use surveillance cameras for the safety and security of the school, 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.

The data protection principles

Data collected from 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 that 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 UK-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.

Objectives

The CCTV system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.

- Deter criminal acts against persons trying to enter the school.
- Assist the police in identifying persons who have committed an offence.

Protocols

The CCTV system will be registered with the ICO in line with data protection legislation. The CCTV system is a closed digital system. Warning signs have been placed throughout the premises where the CCTV system is active, as mandated by the ICO's Code of Practice.
The CCTV 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 CCTV system will not be trained on individuals unless an immediate response to an incident is required. The CCTV system will not be trained on private vehicles or property outside the perimeter of the school.

Security

Access to the CCTV system, software and data will be strictly limited to authorised operators and will be password protected.

The school's authorised CCTV system operators are:

- The Head Teacher
- The School Business Manager
- The School Premises Officer

Authorised users will be required to abide by this policy at all times. The main control facility will be kept secure and locked when not in use. CCTV systems will be tested for security flaws once a month to ensure that they are being properly maintained at all times. CCTV systems will not be intrusive.
The DPO and Head Teacher will decide when to record footage but at present, this is deemed as unnecessary because the system only covers the entry to the school, allowing staff to identify those who wish to gain entry.

The school's CCTV system can record audio within the main reception area, but the buzzer entry system is preferred, in conjunction with the images that are generated.

Any cameras that present faults will be repaired immediately so as to avoid any risk of a data breach. Visual display monitors are located in the school. The areas holding these are locked when not in use.

Privacy by design

The use of CCTV will be critically analysed using a Data Protection Impact Assessment (DPIA). A DPIA will be carried out prior to the installation of any surveillance and CCTV system. 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.

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 Privacy Notices.

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 Head Teacher and School Business Manager are responsible for keeping the records secure and allowing access. The default is for the system **not** to record.

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, 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, volunteers and law enforcement.
- Be accurate and well maintained to ensure information is up to date.

Image storage procedures

In order to maintain and preserve the integrity of any digital records, including USB sticks or a hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

- Each USB stick must be identified by a unique reference number (UIS001, UIS002 & UIS003).
- Before use, each USB stick must be cleared of any previous recording.
- The person responsible for recording will register the date and time of USB stick recordings, including the unique reference number.
- All USB sticks required for evidential purposes must be sealed, witnessed, signed by the person responsible for recording, dated and stored in the safe. If a USB stick is not copied for the police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the responsible member of staff, dated and returned to the safe.
- If the USB stick is archived, the reference must be noted.
- USB sticks may be viewed by the police for the prevention and detection of crime. A record will be maintained of the release of USB sticks to the police or other authorised applicants. A register will be available for this purpose.
- Viewing of USB sticks by the police or any external individual must be recorded in writing and entered in the register. Following an appropriate Subject Access Request from the police, USB sticks will only be released to the police on the clear understanding that the data remains the property of the school, and both the USB stick and information contained on it are to be treated in accordance with this code. The school also retains the right to refuse permission for the police to pass to any other person the USB stick or any part of the information contained thereon. On occasions, when a court requires the release of an original USB stick, this will be produced from the safe, complete in its sealed bag. The police may require the school to retain the stored USB sticks for possible use as evidence in the future. Such USB sticks will be properly indexed, properly and securely stored until they are needed by the police.

- Applications received from outside bodies (e.g. solicitors) to view or release USB sticks will be referred to the Head Teacher. In these circumstances, USB sticks will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a Subject Access Request, or in response to a court order. This must be provided within one month of receiving the request. If the decision is taken not to release the images, then the image in question should be held and not destroyed until all legal avenues have been exhausted.

Access

Under the UK-GDPR, individuals have the right to obtain confirmation that their personal information is being processed. All disks containing images belong to, and remain the property of, the school.
Individuals have the right to submit a Subject Access Request 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 a 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 Head Teacher, 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, excessive or repetitive, a reasonable fee will be charged.
- All fees will be based on material cost of providing the information. For example, memory sticks or disks.
- All requests received during school term time will be responded to without delay and within one month of receipt. Requests received during school holidays may not be able to be responded to in this timeframe but will be responded to as soon practicable.
- 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.
- 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 Head Teacher will make the final decision as to whether recorded images may be released to persons other than the police.

Monitoring and Review

This policy will be monitored and reviewed on an annual basis by the Head Teacher and senior leaders with advice from the DPO. The Governing Body will ratify the policy following review.

The school will monitor any changes to legislation that may affect this policy, and make the appropriate changes accordingly. The Head Teacher or School Business Manager will communicate changes to this policy to all members of staff.

Signed: _____ (Chair of the Governing Body)

Date: _____

Signed: _____ (Head Teacher)

Date: _____