Marriott Primary

Achieving Together

CCTV POLICY

Approved	**15th June 2021**
Signed **(Chair of Governors)**	***Steve Wilson***
Reviewed (Due: 15th June 2024)	
Signed **(Chair of Governors)**	

Contents

Background

In order for Marriott Primary School (MPS) to comply with the requirements of the UK General Data Protection Regulations (GDPR), the Data Protection Act 2018, the Information Commissioners CCTV Code of Practice and the Protection of Freedoms Act 2012 the school must have a policy on its use of CCTV.

The scope of this Policy applies to all MPS employees and Governors. In addition, all agency workers, partner agencies' contractors and vendors who are required to use MPS information systems will also be made aware of and be expected to comply with this policy. This policy forms part of a suite of Information Governance policies.

This policy and the supporting guidance confirms how the MPS manages its CCTV system, determines who has access to the CCTV data and under what circumstances, including the procedures that will be followed in regard to providing access to CCTV Data.

This document must be read in combination with the Information Commissioner's "CCTV Code of Practice" (Revised Edition) 2008, the Surveillance Camera Code of Practice issued by the Secretary of State pursuant to Section 30 of the Protection of Freedoms Act 2012 and the MPS Data Protection Policy.

Governance

MPS recognises that recording images of identifiable individuals is processing personal information within the requirements of the Data Protection legislation. The school notifies all pupils, staff and visitors of the purpose for collecting surveillance data via Privacy Notices and by clear signage around our premises.

The CCTV System owned and operated by MPS complies with the following legislation:

1. UK General Data Protection Regulation
2. Data Protection Act 2018
3. Human Rights Act 1998
4. Protection of Freedoms Act 2012
5. Freedom of Information Act 2000
6. Regulatory and Investigatory Powers Act 2000

Purpose

This document sets out:

i. the basis for these operations;
ii. how MPS's CCTV system (the system) will be controlled and managed in compliance with Data Protection requirements.

The policy will be reviewed periodically by our Data Protection Officer (DPO) to ensure that it continues to meet the public interest test and complies with the necessary legislative requirements.

Objectives

The lawful basis for the use of the system is within our public task as a Primary School and our Legitimate Interests. The objectives of the systems are to:

i. Increase personal safety and reduce the fear of crime for our pupils, parents, the public and our staff.
ii. Support the Police in the prevention and detection of crime.
iii. Assist in the identification, apprehension and prosecution of offenders.

iv. Where appropriate monitoring our staff and standards including our Health & Safety responsibilities. and procedures
v. Protect our key buildings and their assets.
vi. Monitoring pupil movement and behaviour.

Statement of Intent

The CCTV System is registered with the Information Commissioner and is operated in accordance with the requirements of the UK GDPR and the Commissioner's Code of Practice. MPS will treat the information obtained by the system as personal data protected under the data protection and UK GDPR legislation.

Our system may also be used to monitor activities to identify potential criminal activity or anti-social behaviour occurring, anticipated, or perceived, for the purpose of securing the safety and reassurance of the public or security of MPS and council property.

CCTV surveillance is maintained using CCTV cameras in fixed positions. CCTV cameras are not focussed on nor intended to monitor or record any behaviour in adjacent private homes, gardens or other areas of private property.

Data or knowledge secured as a result of MPS CCTV will not be used for any commercial purposes. Data will only be released to the Police for use in the investigation of a specific crime upon receipt of appropriate written request from the police (see below).

Data will not be released directly to any media representative unless our DPO or the police confirm that it would be in the public interest to do so or it is required to defend any legal challenge or intended legal action.

The planning and design of the system aims to ensure that it will give maximum effectiveness and efficiency, but it cannot guarantee to cover or detect every incident taking place in the areas of coverage.

Appropriate signage, as required by the Information Commissioners has been placed in key locations in the areas covered by the CCTV.

Operation of the System

The Scheme is managed by MPS in accordance with this policy and the principles and objectives expressed in this and related policies and procedures.

Day to day administration of the system will be the responsibility of MPS.

The CCTV system will operate continuously 24 hours a day, each day subject to operational considerations such as maintenance and repair.

Control of Equipment

The system will be periodically checked to confirm the efficiency of the system ensuring the equipment is properly recording and the CCTV operational. Any cameras that present faults will be repaired immediately so as to avoid any risk of a data breach.

Access to the system

Access to the system and equipment will be restricted to the school's authorised CCTV system operators:

i. Headteacher and Deputy
ii. Business Manager
iii. School Premises Officer
iv. DPO
v. our CCTV maintenance contractors and associated staff.

Viewing of the recordings is restricted to the above authorised personnel to access and view the images, this includes the Police for the prevention and detection of crime. Appropriate evidence and grounds will be required before any access is allowed. A register of access is maintained by the MPS Business Manager. Full details of each access that has taken place shall be recorded including name, reason for request, staff involved in access and viewing, time and date.

If a serious incident is viewed on the system by MPS staff, the appropriate emergency services will be requested.

Recordings from the cameras will only be routinely retained for a period of 30 days. Where images are requested to be secured by the police for possible future action to detect or prevent crime this may be agreed by the school DPO. Where images are required for possible Court action, guidelines and requirements under the Criminal Procedure and Investigations Act 1996 will be followed (see below 'Recordings handed to the police/used in evidence'). Please consult the school DPO for further advice.

Systematic checks must be carried out to ensure compliance with the agreed retention period. When the documented period of retention has been reached images must be removed and erased. However, any images that are to be retained as evidence must be kept in a secure location with controlled access.

Viewing data

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. The DPO and Headteacher will decide when to record footage e.g. a continuous loop outside the school grounds to deter intruders. Any unnecessary footage captured will be securely deleted from the school system.

The school's CCTV system will record **audio** within the main reception area.

Visual display monitors are located within the main office and may be switched off when required to prevent unnecessary viewing of images. These areas are locked when not in use.

Recordings handed to the police/used in evidence

In order to maintain and preserve the integrity of recordings, USB/CD/DVD's used to record events and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:

i. Each USB/CD/DVD must be identified by a unique exhibit number/mark.
ii. The CCTV operator shall register the date and time and reference title of the USB/CD/DVD and who it or any copies was handed to in a CCTV recordings log.

A recording required for evidential purposes must be sealed, witnessed, signed by the operator, dated and stored in a separate, secure, evidence store. If a USB/CD/DVD 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 controller, dated and returned to the evidence USB/CD/DVD store.

A record will be maintained of the release of copies of recordings to the Police or other authorised applicants in the CCTV log.

Viewing of recordings by the Police must be recorded in writing. Requests by the Police can only be actioned in accordance with the UK GDPR. On occasions the Police may require urgent access to the system, for example to protect human life, or minimise serious damage and injury or when searching for offenders or missing persons. On such occasions urgent, spontaneous access may be permitted but a record of the time/date and details recorded.

Should a USB/CD/DVD be required as evidence, a copy may be released to the Police under the procedures described above. USB/CD/DVD will only be released to the Police on the clear understanding that the USB/CD/DVD remains the property of MPS, and both the USB/CD/DVD and information contained on it are to be treated in accordance with this policy. MPS also retains the right to refuse permission for the Police to pass to any other person the USB/CD/DVD or any part of the information contained thereon. On occasions when a Court requires the release of an original USB/CD/DVD this will be produced from the secure evidence USB/CD/DVD storage area still complete in its previously sealed bag.

The Police may require MPS to retain the stored USB/CD/DVDs for possible use as evidence in the future. Such USB/CD/DVDs will be properly indexed and properly and securely stored until they are required by the Police.

Applications received from any individuals or external bodies (e.g. solicitors) to view or release USB/CD/DVDs will be referred to the MPS DPO. In these circumstances USB/CD/DVDs may 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.

Training

All staff involved in operating the equipment must be trained in Privacy legislation and able to recognise a request from a member of the public for access to recorded images.

Subject Access Requests

The UK GDPR provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including images obtained by CCTV. The MPS DPO must be consulted as soon as possible when such requests involve CCTV recordings.

Breaches of this policy

Any breach of this policy will be initially investigated by the MPS DPO, in order for appropriate action to be taken. A report of the incident will be made to the MPS Head teacher together with any recommended actions to remedy the breach.

Note: A serious breach of this policy may lead to disciplinary action.

Any serious breach of the policy may be further investigated by an independent investigator reporting on recommendations to remedy the breach (consider BLS who are experienced at such reviews).

Review of use of the system

Performance monitoring, including random operating checks, may be carried out by any of the above-mentioned authorised staff at any time.

Complaints

Any complaints about the MPS use of its CCTV system should be addressed to the MPS DPO.

Public information

Copies of this policy should be made available to the general public via MPSs website or in paper form from the MPS DPO.