


Proud to be a Bright Futures EDUCATIONAL TRUST school

Marton Primary Academy and Nursery



Working Together To Be The Best We Can Be

CCTV Policy

**Approved by the Governing Body
22nd November 2021**

MARTON PRIMARY ACADEMY AND NURSERY CCTV POLICY

'Working together to be the best we can be.'

Purpose

The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Marton Primary Academy and Nursery (MPA). The system comprises a number of fixed cameras located within and around the school buildings. The system can only be accessed by nominated staff. Bright Futures Educational Trust (BFET) owns the CCTV system.

This policy should be read in conjunction with the Trust Data Protection Policy and our privacy notices.

CCTV System

The Data Controller of the data held in the system is BFET.

The Local Governing Board considers that the CCTV system contributes to security and the health and safety of pupils, staff and visitors. The Head of School and Governors have considered the need for using a CCTV system and have decided that it is required for the prevention of crime and for protecting the safety of pupils, staff and visitors to the site. In the event that the CCTV captures an incident which is relevant evidence for an internal process or required by a competent authority to BFET fully reserves its right to use the footage during its internal process or share it as may be lawfully permitted.

The general management of CCTV at Marton Primary Academy and Nursery is currently vested with the Hub Operations Manager. The day-to-day management and operation of the CCTV system is the responsibility of the Site Staff.

The Primary Purposes of Marton Primary's Use of CCTV

CCTV system is installed (both internally and externally) in the 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 Marton Primary Academy and Nursery is intended for the purposes of:

Complying with our public duty to keep children in our care safe;

- To increase personal safety of pupils, staff and visitors and reduce the fear of crime;
- To protect the buildings and their assets;
- To protect members of the public and private property;
- To improve security and to detect persons who are not authorised to be on the premises;
- To support police in a bid to deter and detect crime;
- To assist in identifying, apprehending and potentially prosecuting offenders;
- To identify individuals including pupils and staff engaged in improper conduct.

Statement of Intent

This policy has been drafted in accordance with the Information Commissioner's '*In the picture: A data protection code of practice for surveillance cameras and personal information*'. BFET is registered as a fee paying Data Controller with the Information Commissioner's Office in accordance with the GDPR 2016. This Policy follows the GDPR 2016 and Data Protection Act 2018. The school will treat the system and all information, documents and recordings obtained and used as data protected by the law.

Cameras will be used to monitor activities within the school and the grounds to identify adverse activity actually occurring, anticipated or perceived, and for the purpose of securing the safety and well-being of the school's pupils and staff, together with its visitors.

Static cameras are positioned to ensure they do not focus on private homes, gardens and other areas of private property. At no time will a camera be directed to follow or track an individual.

Materials or knowledge secured as a result of CCTV use will not be used for any commercial purpose. Images will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that the CCTV system will give maximum effectiveness and efficiency within available means, but it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Warning signs to be alert to the use of CCTV, as required by the Code of Practice of the Information Commissioners Office, have been placed at all access routes to areas covered by the school's CCTV system.

Location of Cameras

The location of CCTV cameras is based upon a variety of information including security, health and safety and safeguarding.

The cameras are sited so that they only capture images relevant to the purposes for which they have been installed, and care will be taken to ensure that reasonable privacy expectations are not violated. MPA will ensure that the location of equipment is carefully considered to ensure that the images captured comply with the legislation. MPA will make every effort to position the cameras so that their coverage is restricted to the premises, which includes both indoor and outdoor areas.

All such CCTV equipment installed in the building will only be sited in such a way that it only monitors those spaces that are intended to be covered by the equipment.

If domestic areas such as gardens or areas not intended to be covered by the system border those spaces which are intended to be covered by the equipment, then Marton Primary Academy and Nursery shall consult with the owners of such spaces if images from those spaces might be recorded. In the case of back gardens, this would be the resident of the property overlooked.

The employees and pupils will be made aware of the purpose (s) for which the system has been established and notices to this effect will be displayed in the school reception area and the hallways. Parents will be informed via the promotional materials provided by each school.

The operators will only use the equipment in order to achieve the purpose(s) for which it has been installed.

Cameras that are adjustable by the operators will not be adjusted or manipulated by them to overlook spaces which are not intended to be covered by the scheme, other than as described in this policy.

If it is not possible physically to restrict the equipment to avoid recording images from those spaces not intended to be covered by the system, then operators will be trained in recognising the privacy implications of such spaces being covered.

Internal cameras are located in general circulation areas with the exception of the cameras located to view the washbasin areas in the student toilets to reduce vandalism. Pupil privacy is not compromised by the latter.

Operation of the System

The CCTV system will be managed by the Hub Operations Manager, in accordance with this policy and any applicable Code of Practice issued by the ICO. The day-to-day management will be the delegated responsibility of the Site Staff on duty. The CCTV system will operate 24 hours each day, every day of the year, recording all activity.

Use of Audio

The ICO states that the use of audio can be justified in limited circumstances and those operators should not “listen in”.

The current CCTV system installed in school records visual images only and is not an audio system.

Staff Authorised to Operate the CCTV System

The Hub Operations Manager, site staff and the senior leadership team.

Staff Authorised to View CCTV Footage

The Executive Principal, the Head of School, the Safeguarding Team and those authorised to operate the system (listed above) are permitted to view CCTV footage or still pictures. In addition, Governors, or senior leaders who sit on exclusions, disciplinary/grievance panels will view CCTV images if relevant to the process being investigated and subject to determination. Persons not named must seek authorisation from the Head of School. This includes all members of staff and police officers. The police are able to use footage for evidence following an incident providing prior permission has been agreed with the Head of School. A DP form must be completed and an electronic copy of the document will be held by the data protection co-ordinator. In the event that a request is not clear the data protection co-ordinator must refer the matter to the Data Protection Officer for advice.

Access to Recorded Images

Viewing of the recorded images should take place in a restricted area or designated member of staff's office. Other employees will not be allowed to have access to that area when a viewing is taking place.

All operators should be trained in their responsibilities under the Code of Practice, i.e. they should be aware of:

- The user's security policy e.g. procedures to have access to recorded images;
- The user's disclosure policy

The main CCTV system in the Site Supervisor's office is password protected and only authorised staff have passwords to gain access to recorded images.

Access to Live Images

Monitors displaying images from areas in which individuals would have an expectation of privacy should not be viewed or be capable of being viewed by anyone other than authorised persons.

Viewing of live images should only be carried out when there is a suspicion that improper conduct may be carried out at a particular time.

The privacy of staff and pupils going about their normal legitimate business must be respected at all times.

Quality of Images and Storage of Recorded Material

Upon installation an initial check will be undertaken to ensure that the equipment performs properly. Regular checks will be made thereafter to ensure that the system is operating properly.

Images are retained on the server for up to 30 days. However, copies may be made for investigation purposes and will therefore be retained for longer in accordance with the applicable process and retention periods applied to evidence relied upon within such processes.

Checks will be made to ensure the accuracy of any features such as the location of the camera and/or date and time reference. Where the time/date etc. are found to be out of sync with the current time/date, the operators will take such remedial action as is continued in the operations manual to correct the error.

Cameras will only be situated so that they will capture images relevant to the purpose for which the scheme has been established.

When installing cameras, consideration will be given to the physical conditions in which the cameras are located.

Cameras will be properly maintained and serviced to ensure that clear images are recorded.

Servicing will be carried out at least annually.

Cameras should be protected from vandalism in order to ensure that they remain in working order.

A maintenance log will be kept in the monitoring centre of the system concerned.

The Hub Facilities Manager will be:

- The person responsible for making arrangements for ensuring that a damaged camera is fixed.
- Ensuring that the camera is fixed within a specific time period.
- The person responsible for monitoring the quality of the maintenance work.
- Once the retention period has expired, ensuring the images are removed or erased.
- Ensuring the images that are to be retained for evidential purposes will be retained in a secure place to which access is controlled.

Access to and disclosure of images to third parties

Access to recorded images will be restricted to those persons who need to have access in order to achieve the purpose(s) of using the equipment.

All access to the medium on which the images are recorded should be documented.

Disclosure of the recorded images to third parties should only be made in limited and prescribed circumstances. Disclosure will be limited to the following classes of persons/agencies.

- Law enforcement agencies, where the images recorded would assist in a specific enquiry.
- Highways authorities in respect of traffic management matters.
- Law enforcement agencies where the images would assist a specific criminal enquiry.
- Local authority where the image may be relevant to an investigation being conducted in accordance with a statutory duty or pursuant to a power granted to the Local Authority.
- Prosecution Agencies.
- Relevant legal representatives.

All requests for access or for disclosure in accordance with our data protection requirements and on completion of our DP release form should be recorded, if access or disclosure is denied, the reason should be documented.

If access to or disclosure of the images is allowed, then the following will be documented.

The date and time at which access was allowed or the date on which disclosure was made.
The identification of any third party who was allowed access or to whom disclosure was made

The reason for allowing access or disclosure;

Location of the images

Any crime incident number to which images may be relevant

Signature of person authorised to collect the medium – where appropriate

Any advice provided by the Data Protection Officer and/or BFET's professional advisors.

Recorded images will not be made more widely available – for example they should not be routinely made available to the media or placed on the Internet.

Breaches of the policy (including breaches of security)

The Head of School, or senior leader acting on their behalf, will initially investigate any breach of the CCTV policy by school staff. Any serious breach of the policy will be subject to the terms of disciplinary procedures already in place. Any potential breaches of Data Privacy will be immediately reported to the Trust's Data Protection Officer.

Subject Access Request by data subject (SAR)

The GDPR provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about them, including those obtained by CCTV. Requests for Data Subject Access should be made through the academy's Data Protection Co-ordinator or the Trusts Data Protection Officer.

Data subjects should be provided with a standard subject access request form, a copy of this form is attached.

The above form will also enquire whether the individual would be satisfied with merely viewing the images recorded. The form will also indicate that the response will be provided promptly and in any event within 30 days of receiving.

Individuals, at the time of any SAR, will be given a description of the type of images recorded and retained and the purpose for which the recording and retention takes place.

Prior to any authorised disclosure, the Data Protection Officer will need to determine whether the images of another "third party" individual features in the personal data being applied for and whether these third party images are exempt from disclosure under the Data Protection Act 2018 in accordance with the protection of the rights of others.

If third party images are not to be disclosed the school shall arrange for the third party images to be disguised or blurred. In some cases, obscuring will not be achievable and the image may be withheld from disclosure.

If the Data Protection Officer decides that a SAR from an individual is not to be complied with they will document this.

Complaints

Any complaints about the schools CCTV system should be addressed to the Head of School.

Appendix 1

Form to request access to CCTV images

Name:

Address:

Telephone Number:

Date of Birth:

Date image recorded:

Time image recorded:

Description of image recorded (if relevant):

The Data Protection Officer will consider the request and respond within 30 days.

Appendix 2

Record of access to CCTV images

Name of authorised staff member(s)

Date and time of access

Name of any third party who was allowed access

The reason for allowing access

Location of the images

Any crime incident number to which images may be relevant

Signature of person authorised to collect the medium (if relevant)

Any advice provided by the Data Protection Officer and/or BFET's professional advisors.