



# CCTV Policy

Reviewed	Date of Next Review	Responsibility
February 2024	February 2026	Head of Finance

## Our Mission:

**'To enable young people to live and work without barriers'**

## Our Values:

- **Teamwork** – we hold ourselves and each other to account and are better when we work together
- **Compassion** – we act with trust, honesty and kindness in everything we do
- **Inclusion** – we treat each other fairly and with respect
- **Innovation** – we encourage thoughtful, creative and aspirational ideas
- **Pride** – we encourage each other to be proud of who we are and what we do

## **Introduction**

The purpose of this document is to regulate the management, operation, and use of CCTV systems across the Trust.

The Trust uses closed circuit television (CCTV) images to reduce crime and monitor the academy buildings in order to provide a safe and secure environment for pupils, staff, and visitors, to prevent the loss or damage to property and to assist in the investigation of accidents, incidents and near misses.

The system comprises of both fixed and dome cameras, some are electronically moveable and are located on walls and ceilings in the buildings.

The CCTV system is owned and operated by the Trust and the deployment of the cameras is determined by the CEO.

The use of CCTV, and the associated images, is covered by the Data Protection Act 1998. This policy outlines the Trust's use of CCTV and how it complies with the Act.

All authorised operators and employees approved to access images are aware of the procedures that need to be followed when accessing the recorded images and sound. All operators are trained by the Trust in their responsibilities as part of the requirements of this policy document, the Trust's Safeguarding policies and procedures, E-Safety information, and the Data Protection Act. All employees are aware of the restrictions in relation to storage of, access to, and disclosure of, recorded images and sound. Failure to adhere to these requirements could lead to disciplinary action.

## **Statement of Interest**

The Trust complies with Information Commissioner's Office (ICO) CCTV Code of Practice to ensure it is used responsibly and safeguards both the Trust and confidence in its continued use.

CCTV warning signs will be clearly and prominently placed at all external entrances to the buildings on the sites where CCTV is deployed. Signage will contain details of the purpose for using CCTV.

The planning and design of the system should minimise any invasion of privacy and ensure that the scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the system will fully meet this brief or detect every single incident taking place in the areas of coverage.

CCTV data will not be used in any aspect of performance management, unless with the written consent of the employee concerned.

## **Siting of Cameras**

Cameras will be sited so that where possible, they only capture images relevant to the purposes for which they are installed (described above) and care will be taken to ensure that civil rights and privacy are not violated. Consideration of position will ensure that the location of equipment enables captured images to comply with the Data Protection Act, cameras will be regularly checked to ensure they have not been moved or tampered with in any way.

The Trust will make every effort to position cameras so that their coverage is restricted to the Trust's premises, which will include outdoor areas.

CCTV will not be used in classrooms but may be used in areas that are considered to be susceptible to inappropriate use or abuse. CCTV will not be used inside any residential areas.

Members of staff upon request will have access to details of where CCTV cameras are situated, with the exception of cameras placed for the purpose of covert monitoring (see section on Covert Monitoring).

## **Operation of the System**

The CEO of the Trust is responsible for the operation of the CCTV system and for ensuring compliance with this policy.

Breaches of the policy by staff monitoring the system may constitute a disciplinary matter under the relevant conditions of employment.

Any concerns in respect of the system's use or regarding compliance with this policy should be addressed to the CEO.

The system will be administered by MSA 365 along with relevant authorised staff; working in accordance with the principles and objectives expressed in this policy.

The CCTV system will be in operation 24 hours each day, for every day of the year.

A nominated person will check on a weekly basis that the system is operating effectively and in particular that the equipment is properly recording and that cameras are functional.

The system will be regularly serviced and maintained.

### **Use of Data**

The CCTV System will be used for the purpose of:

- The prevention, detection, and investigation of criminal activity.
- The security of the premises.
- Safeguarding the safety of young people, staff, and visitors

### **Covert Monitoring**

Covert monitoring should not normally be considered, and should only be used in exceptional circumstances, for example:

- Where there is good cause to suspect that a criminal activity or equivalent malpractice which may constitute gross misconduct.
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances written authorisation must be obtained from the CEO before allowing such an operation to take place. Unless the CEO is instructed otherwise (e.g. in a police investigation), members of the Trust will be informed confidentially about any plans for covert monitoring.

Covert monitoring must cease following completion of an investigation.

Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets or changing areas.

### **Storage and Retention of CCTV Images**

Recorded data will not be retained for longer than is necessary to meet the purposes of recording them and will be deleted/erased appropriately and in line with approved procedures for the Trust. Video/still images will be held for no longer than 40 days when the system will automatically overwrite the previous data. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.

All data will be stored securely. Access will be limited to named operators/staff only whose access is authorised by the CEO.

### **Access to CCTV Images**

Access to recorded images will be restricted to those staff authorised to view them by the CEO.

Any staff who are authorised to view images from this CCTV system will be listed in this Policy in Appendix 1.

A log will be maintained of when CCTV footage is accessed and reviewed (name of reviewer, date & reason). A template of this log can be found in Appendix 2, the actual log will be an electronic log.

## **Subject Access Requests (SAR)**

Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.

All requests must be made in writing to the CEO. Email is not acceptable. Individuals submitting requests for access will have to provide sufficient information to enable the footage relating to them to be identified & isolated. For example, date, time, and location.

The Trust will respond to requests within 40 calendar days of receiving the written request. At the discretion of the CEO, an administrative fee of £10 may be charged per Subject Access Request (SAR).

The Trust reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an ongoing investigation. Where images of other individuals are on the CCTV footage their permission will be sought before access is allowed.

## **Access to and Disclosure of Images to Third Parties**

There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the Trust where these would reasonably need access to the data (e.g. investigators).

Requests should be made in writing to the CEO.

The data may be used within the Trust's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

## **CCTV Signage**

It is a requirement of the Data Protection Act 1998 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The Trust must ensure that this requirement is fulfilled.

The CCTV signage should include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the Trust
- The contact telephone number or address for enquiries

## **Complaints**

Complaints and enquiries about the operation of CCTV within the trust should be directed in writing (and not via email) to the CEO, Fairfield Trust, 43 High Street, Dilton Marsh, Westbury BA13 4DL.

Failure of authorised operators/staff to comply with the requirements of this policy may lead to disciplinary action under the Trust's disciplinary procedure.

## **Further Information**

Further information on CCTV and its use is available from the following:

- CCTV Code of Practice Revised Edition 2008 (published by the Information Commissioners Office)
- [www.ico.gov.uk](http://www.ico.gov.uk)
- Regulation of Investigatory Powers Act (RIPA) 2000
- Data Protection Act 1998

Approved by the Board.

**Kate Durrant**  
**Head of Finance**

February 2024

**Appendix 1**

CCTV – Use and Disclosure of Images Protocol:

Legitimate public concerns exist over the use of CCTV and many of the specific guidelines are designed to satisfy the community that the use of cameras is subject to adequate supervision and scrutiny. It is of fundamental importance that public confidence is maintained by fully respecting individual privacy. All employees that are authorised to view the CCTV images within the Trust must read this protocol alongside the CCTV Policy and confirm that they understand and agree to abide by the policy and protocol.

CCTV images may only be viewed by authorised employees.

All authorised employees viewing the CCTV images will always act with utmost probity.

All images viewed by **authorised employees** must be treated as confidential.

All authorised employees are to ensure that whilst viewing CCTV images, **unauthorised employees** or visitors cannot view the images.

All authorised employees are responsible to ensure that CCTV images are not left on any screen without an authorised employee being left in charge. An authorised employee should log out of the programme when leaving the screen.

Every viewing of the images will accord with the purposes and key objectives of the CCTV system and shall comply with the CCTV Policy.

All authorised employees viewing CCTV images should be aware of exercising prejudices, which may lead to complaints of the system being used for purposes other than those for which it is intended. The viewers may be required to justify their interest in any particular individual, group of individuals or property at any time.

All authorised employees viewing CCTV images are responsible for their viewing of the images, which must be justifiable.

Any breach of the CCTV Policy or CCTV Protocol will be dealt with in accordance with existing discipline regulations. Individuals must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.

Any breach of the Data Protection Act 1998 will be dealt with in accordance with that legislation. All authorised employees viewing CCTV images must be aware of their liability under this Act.

Authorised users of the system:

Name	Job Title	Date
Vicky Dunncliffe	CEO	February 2024
Graeme Athey	Principal	February 2024
Kate Durrant	Head of Finance	February 2024
Rupert Hughes	Site Manager	February 2024
MSA 365	External IT Contractor	February 2024

