CCTV Policy
Fairfax Multi-Academy Trust

Document Owner:	**Robert Fitzgerald, I&S Manager & DPO**
Ratified By:	**Board of Directors (BoD)**
Date Ratified:	**April 2024**
Review Date:	**April 2027**

Contents

Appendices

1. Policy statement

1.1. This document sets out the appropriate actions and procedures which must be followed to comply with data protection legislation regarding the use of CCTV (closed circuit television) surveillance systems managed by the Trust.

1.2. This policy is intended to assist staff in complying with their own legal obligations when working with personal data captured on CCTV.

1.3. This policy operates in conjunction with the following Trust policies and procedures:

- **Data Protection Policy**
- **Data Breach Procedure**
- **Data Protection Impact Assessment (DPIA) Procedure**
- **Privacy Notices**
- **Retention Schedule**
- **Subject Access Request Procedure**

2. Scope of the policy

2.1. This policy applies to all Trust buildings and estates.

3. CCTV usage

3.1. We currently use CCTV cameras to view and record individuals on and around our premises. This policy outlines why we use CCTV, how we will use CCTV and how we will process data recorded by CCTV cameras to ensure we are compliant with data protection law and best practice.

3.2. We recognise that information that we hold about individuals is subject to data protection legislation. The images of individuals recorded by CCTV cameras in the workplace are personal data and therefore subject to the legislation. We are committed to complying with all our legal obligations and seek to comply with best practice suggestions from the Information Commissioner's Office (ICO).

3.3. This policy covers all employees, contractors, trustees, volunteers, visitors and any other individuals engaged to perform services for the Trust.

3.4. This policy has been reviewed by the Trust Data Protection Officer (DPO) and approved by the Trust's Audit and Risk Committee (ARC). This policy is available on the Trust website.

3.5. The Trust's privacy notices for staff, parents and students include information about the use of CCTV by the Trust, including for what purpose it is used. A copy of the privacy notices can be found on the Trust's website by clicking here.

3.6. Staff approved to access recorded CCTV images, within their permitted activities, are defined in table 1 below.

Table 1 – Staff who can view and/or download Recorded CCTV images:

View and/or Download Recorded CCTV Images:		
1	Principal of Academy	
2	Trust Health and Safety Manager	
3	Trust Estates Manager	
4	Trust Executive Team	
5	Senior Site Team	***Only with the express permission of 1, 2 ,3 or 4 above***
6	IT Support	
8	Other Academy Staff Members	
9	BAM FM (Smith's Wood Academy Only)	
View-only Recorded CCTV Images:		
10	Principal of Academy Representative at SLT	
11	Designated Safeguarding Lead (DSL) and Deputy Designated Safeguarding Leads (DDSL) in the Academy	
12	Other Academy Staff Members	***Only with the express permission of 1, 2,3 or 4 above***

3.7. Only approved staff can access CCTV recordings, and they must complete and receive approval the **CCTV Access Authorisation Form** (see Appendix 1) prior to downloading any CCTV images.

4. Breaches of this policy

4.1. A breach of this policy may, in appropriate circumstances, be treated as a disciplinary matter. Following investigation, a breach of this policy may be regarded as misconduct leading to disciplinary action, up to and including dismissal.

4.2. Any breach of CCTV information, for example, unauthorised access to CCTV footage, must be reported immediately to the Trust's Data Protection Officer (DPO) and will be investigated in accordance with the Trust's **Data Breach Procedure**.

4.3. All authorised employees accessing CCTV footage must ensure the security and confidentiality of the images, such as; not viewing in a public location, saving and footage to a secure location and encrypting files when transferring them.

5. Responsibilities

5.1. Day-to-day management responsibility for deciding what information is recorded, how it will be used and to whom it may be disclosed has been delegated to the those listed in section 3.6, table 1 of this policy.

5.2. Day-to-day operational responsibility for CCTV cameras and the storage of data recorded is the responsibility of the Principal of Academy.

5.3. This policy will be maintained and reviewed at least annually under the supervision of the Trust's Data Protection Officer (DPO) to ensure that the use of CCTV continues to be justified and that the appropriate measures are in place to mitigate data protection risks raised by its use.

6. Purpose of the CCTV system

6.1. We currently use CCTV on our premises for the following reasons:

6.1.1 to prevent crime and protect buildings and assets from damage, disruption, vandalism, and other crime.

6.1.2 for the personal safety of students, staff, visitors, and other members of the public and to act as a deterrent against crime.

6.1.3 to support law enforcement bodies in the prevention, detection, and prosecution of crime.

6.1.4 to assist in the day-to-day management, including ensuring the health and safety of students, staff, and others.

6.1.5 to assist in the effective resolution of disputes which arise in the course of disciplinary or grievance proceedings.

6.2. The items listed in 7.1.1 to 7.1.5 are not exhaustive and other purposes may become relevant.

7. CCTV monitoring

7.1. Cameras are situated to ensure they cover Trust premises as far as is possible, including the exterior of buildings, vulnerable public facing areas, car parks, outside spaces, communal areas within buildings and both the main entrance and secondary exits.

7.2. The CCTV system is currently in operation and capable of being monitored 24 hours a day, every day of the year.

7.3. As far as practically possible CCTV cameras will not focus on private homes, gardens, or other areas of private property.

7.4. Prior to introducing any new surveillance system, including placing a new CCTV camera in any workplace location, and will be carefully considered if they are appropriate through carrying out a **Data Protection Impact Assessment (DPIA)**.

7.5. Any **Data Protection Impact Assessment (DPIA)** will consider the nature of the problem that we are seeking to address at that time and whether the surveillance camera is likely to be an effective solution, or whether a better solution exists. In particular, we will consider the effect a surveillance camera will have on individuals and therefore whether its use is a proportionate response to the problem identified.

8. How we will operate any CCTV system

8.1. We will ensure that signs are displayed at the entrance of the surveillance zone to alert individuals that their image may be recorded. Such signs will contain details of which organisation is monitoring the CCTV (if not wholly operated by the Trust) and who to contact for further information, where these things are not obvious to those being monitored.

8.2. We will ensure that any recorded images are only viewed by those whose role requires them to have access to such data as outlined in section 3.6, table 1. Where relevant, the CEO will make this decision.

8.3. We will never engage in covert monitoring or surveillance (that is, where individuals are unaware that the monitoring or surveillance is taking place) unless, in highly exceptional circumstances, there are reasonable grounds to suspect that criminal activity or equivalent serious malpractice is taking place and, after suitable consideration, we reasonably believe there is no less intrusive way to tackle the issue.

8.4. In the unlikely event that covert monitoring is considered to be justified, the Academy will carry out a **Data Protection Impact Assessment (DPIA)**. The rights of individuals whose images may be captured will always be taken into account in reaching any such decision.

8.5. Trust sites may use visual display screens, these are generally within reception or similar areas to ensure access to the site and main doors are monitored during operational hours. These screens should not be visible to students or members of the public.

9. Use of data gathered by CCTV

9.1. All employees authorised to view CCTV images will act with utmost probity at all times.

9.2. All images viewed must be treated as confidential, and employees must ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images.

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

9.4. CCTV images may only be downloaded by authorised employees or otherwise approved by the relevant member of staff, as stated in section 3.6, table 1.

9.5. No images from CCTV should ever be posted online or disclosed to the media by any member of staff.

10. Retention and erasure of data gathered by CCTV

10.1. Data recorded by the CCTV system will be stored, either on a secure cloud area or a secure server based at the academy.

10.2. Data from CCTV cameras will not be retained indefinitely and deleted automatically from the CCTV system at the earliest opportunity, and within a maximum of 60 days' from the date the recording is made, unless subject to an ongoing incident being investigated or a legitimate access request from a data subject.

10.3. At the end of their useful life, all images stored in whatever format will be erased permanently and securely. Any physical matter such as discs will be disposed of as confidential waste. Any still photographs and hard copy prints will be disposed of as confidential waste.

10.4. Routine checks are made to ensure that the system is operating in accordance with the terms of this policy and that information relating to the recordings (date, time etc.) are accurate.

11. Internal use of CCTV

11.1. If a member of staff considers that CCTV footage might be needed for an internal matter (e.g. a student disciplinary issue) they should speak to the Principal of Academy in the first instance.

11.2. If they are required to download CCTV recordings, they must complete the **CCTV Authorisation Form in (see appendix 1)**.

11.3. Any sharing of these CCTV recordings must be approved by the Principal of Academy, or if unavailable, the Trust's Executive Team.

12. Requests for access and disclosure of CCTV recordings

12.1. Access will only ever be permitted to authorised employees for the purposes of performing their job role within Trust.

12.2. Downloading CCTV images is strictly controlled and limited as set out in section 3.6, table 1 of this policy.

12.3. No images from our CCTV cameras will be disclosed to any third party, without express permission being given by the Principal of Academy and in accordance with data protection requirements.

12.4. Any queries or concerns relating to the sharing of CCTV recordings should be raised with the Trust's Data Protection Officer (DPO).

12.5. Any recordings which are shared with third parties will be shared securely and encrypted whenever possible.

12.6. The academy will maintain a record of all disclosures of CCTV footage and imagines in the **CCTV Log Book (see Appendix 2).**

13. CCTV requests from law enforcement agencies

13.1. In other appropriate circumstances, we may allow law enforcement agencies to view or remove CCTV footage where this is required in the detection or prosecution of crime. Only written requests made under Schedule 2 Part 1 Para. 2 Data Protection Act 2018 (previously Section 29 Request) will be considered.

13.2. Such requests must specify the date and time (as far as possible) of the images required. If CCTV footage is disclosed to a law enforcement agency the academy will record what information has been disclosed, when the disclosure was made, to whom it was disclosed and for what purpose(s) in the **CCTV Log Book (see Appendix 2)**. If the decision is taken not to release the images, then the image in question will be held and not destroyed until all legal avenues have been exhausted.

13.3. Data will not normally be released unless satisfactory evidence that it is required in connection with legal proceedings or if a court order has been produced.

14. Subject access requests (SARs)

14.1. Data subjects may make a request for disclosure of their personal information (known as a data subject access request or subject access requests) and this may include CCTV images.

14.2. In order for us to locate relevant footage, any requests for copies of recorded CCTV images must include the date and time of the recording, the location where the footage was captured and, if necessary, information identifying the individual.

14.3. If the footage contains images of other individuals, then the Academy must consider whether:

14.3.0 The request requires the disclosure of the images of individuals other than the requester, for example whether the images can be distorted so as not to identify other individuals;

14.3.1 The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or

14.3.2 If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.

14.4. The **Subject Access Request (SAR) Procedure** details the requirements for completing a subject access request. Any queries or concerns relating this must be discussed with the Trust's Data Protection Officer (DPO).

15. Complaints

15.1. If any member of staff has any questions concerns about our use of CCTV, they should contact the Principal of Academy in the first instance.

15.2. If any member of the public has any concerns about our use of CCTV, they should contact the Principal of Academy in the first instance.

15.3. Where this is not appropriate or matters cannot be resolved informally, complaints should use our formal Complaints Procedure which is located on the Trust website.

16. Requests to prevent processing

16.1. In rare circumstances, individuals may have a legal right to object to processing and in certain circumstances to prevent automated decision making (see Articles 21 and 22 of the General Data Protection Regulation). For further information regarding this, please contact the Trust's Data Protection Officer at dpo@fmat.co.uk.

Appendix 1 – CCTV Download Authorisation Form

Please complete this form to request downloading of CCTV footage.

This form must be completed by the Principal of Academy. If they are absent the form can be approved by the Trust's Estates Managers or the Trust's Executive Team (ET). See section 3.6, table 1 of the CCTV policy for more details.

1. Requestors Details:

Name:		**Staff initials:**	
Job title:		**Date of request:**	

2. Description of Request:

Date of footage required:		**Time and duration and time of footage:**	
Reason for the request: (Please explain the need to download this footage)			
Where is the Data to be stored?		**Is this request to share with a third party?**	

3. Approval Details:

Approvers Name:		**Approvers Job Title:**	
Request Approved:		**Reason for approval?**	
Date of Approval:		**DPO consulted:**	

This form must be completed prior to the CCTV footage being download. This form must be retained by the academy and recorded on the CCTV Log Book, see Appendix 2

Appendix 2 – CCTV Log Book

Each academy must keep a CCTV Log Book to detail requests to access and download CCTV images.

FMAT CCTV Log Book

Academy:		Document Owner:		Date updated:	

Details of Requestor				Details of CCTV Footage						Approval Details					
Name:	Staff initials:	Job Title	Date of request:	Date of footage required:	Time and duration and time of footage:	People Involved in footage	Reason for the request:	Where is the Data to be stored?	Is this request to share with a third party?	Approvers Name:	Approvers Job Title:	Request Approved:	Justification for approval:	Date of Approval:	Date Request Completed:

The CCTV Logbook template is available in Excel format from the Trust.

The Log Book must be kept up-to-date and be available for review by the Trust's Data Protection Officer (DPO) if required.

Appendix 3 - BAM FM Role with CCTV Images

1.1. At Smiths Wood Academy, the school buildings are operated and managed by a separate facilities management company, BAM FM, under a PFI Contract with the Local Authority. BAM FM is in turn, a sub-contractor of BAM PPP Ltd, one of two parties to Solihull BSF Schools Ltd, which operates and manages the Academy campus under a PFI regime.

1.2. As there is no direct contractual link between Smiths Wood Academy and BAM, a separate side letter has been issued to allow BAM FM, as "data processor" to take instruction directly from Smiths Wood Academy in regard to the capture of CCTV images.

1.3. The Academy buildings are operated and managed by BAM FM. On a day-to-day basis, BAM FM's Facilities Manager and FM staff are responsible for ensuring the appropriate and effective use of the CCTV system and all cameras, data collection and retention processes will be managed by BAM FM.

1.4. BAM FM has their own generic CCTV policy in place to cover their obligations under the GDPR, as well as compliance with the Information Commissioners Office (ICO) CCTV Code of Practice.

1.5. Under the provisions of the GDPR, BAM FM is the Processor of Information held and/or recorded on the CCTV schemes operated by BAM FM. The Trust is the data controller who has the full authority to decide how and why personal data is to be processed and or released. Therefore, BAM FM has no authority to allow access to the CCTV System, other than with the agreement of Smiths Wood Academy.

1.6. Any footage that is recorded and released can only be released to Smiths Wood Academy or the Trust, as data controller. This includes the release of footage to Enforcement Agencies (Police) and BAM FM will refer all requests for access to CCTV images, from whatever source, to the Principal of Academy or the nominated representative, similarly, the BAM FM staff will inform the Principal of Academy, or the nominated representative, of any CCTV footage that appears to show individuals involved in criminal or suspicious activity.