The Park Federation
ACADEMY TRUST

CCTV Policy

Approved by	Helen Abell CEO		
Date	September 2026	**Next review due**	09/2027

Summary of Changes

Version	Date	Summary of Changes	Approved By
1	11th July 2022	Reflects Surveillance Camera Code of Practice (2021) guidance.	Dr Martin Young CEO
2	01 September 2023	Following refurbishment at James Elliman and Wood End Park Academies	Dr Martin Young CEO
3	27 February 2024	Includes Iver Village Infant academy (IVIA)and Hannah Ball academy	Dr Martin Young CEO
4	July 2024	No changes	Dr Martin Young CEO
5	August 2025	Number of cameras for IVIA changed	Dr Martin Young CEO
6	August 2026	Based on the Key model policy approved by Forbes.	Helen Abell CEO

Contents

Heading	Page
Aims	
Relevant legislation and guidance	
Definitions	
Covert surveillance	
Number of cameras	
Roles and responsibilities	
Operation of the CCTV system	
Storage of CCTV footage	
Access to CCTV footage	
Data protection impact assessment (DPIA)	
Security	
Complaints	
Monitoring	
Links to other policies	
Appendix A: Subject Access Request	

Appendix B: Internal Access Request	

1. Aims

This policy is approved by Board Directors of the Park Federation Academy Trust and aims to set out our approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems across our academies. The CCTV system is registered with the Information Commissioners office.

Organisation name: The Park Federation Academy Trust

Registration reference: ZA098238

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the academy community feel safe
- Protect members of the academy community from harm to themselves or to their property
- Deter criminality in the academy
- Protect academy assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

In the unlikely event that the police request that CCTV footage, be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

The footage generated by the system should be of good enough quality to be of use to the police or the court in identifying suspects.

2. Relevant legislation and guidance

This policy is based on:

2.1 Legislation

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- 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

2.2 Guidance

- Surveillance Camera Code of Practice (2021)

3. Definitions

Surveillance: the act of watching a person or a place

CCTV: closed circuit television; video cameras used for surveillance

Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

4. Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed, (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed in order to comply with data protection law.

5. Number of cameras

Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (stated in section 1.1).

The following number of Cameras are located in our academies:

Recording media type: Digital Recorder DVR recording system					
The system records images from: Colour and Black and White cameras					
Academy	**Monitors**	**Fixed cameras**	**Moveable cameras**	**Covert cameras**	**CCTV signs**
Cranford Park	05	73	0	0	16
Hannah Ball	02	08	0	0	2
Iver Village Infant	03	14	0	0	2
James Elliman	04	77	0	0	12
Lake Farm Park	03	38	0	0	10
Montem	01	71	0	0	16
Western House	03	54	0	0	12
Wood End	04	120	01	0	12
Godolphin Junior	03	41	0	0	07
West Drayton	02	57	0	0	12

Wherever cameras are installed appropriate signage is in place to warn members of the academy community that they are under surveillance. CCTV signs are erected around the building within prominent locations that clearly identifies that CCTV recording is in operation. Signs are located at the entrance gate, the building entrance and inside reception.

Cameras are not and will not be aimed off academy grounds into public spaces or people's private property.

Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

6. Roles and responsibilities

6.1 Board of Directors

The Board of Directors have the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Principal

The Principal will:

- Take responsibility for all day-to-day leadership and management of the CCTV system at their academy
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified

- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the academy is compliant with legislation
    - Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the Head of Estates, Specialist contractor or DPO in the use of the system and in data protection
    - Decide, in consultation with the Head of Estates and DPO, whether to comply with disclosure of footage requests from third parties

6.3 The data protection officer

The data protection officer (DPO) will:

- Ensure staff with authorisation to access the CCTV system and footage in the use of the system and in data protection are appropriately trained
- Train all staff to recognise a subject access request
- Deal with subject access requests in line with the UK GDPR and Data Protection Act 2018
- Monitor compliance with UK data protection law
- Advise on and assist the Trust/academy with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office
- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure through the Head of Estates and Premises Teams that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual’s reasonable right to privacy in public spaces
- Carry out periodic checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage

6.4 The system manager

The system manager, Head of Estates, will:

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly

7. Operation of the CCTV system

The CCTV system will be operational 24 hours a day, 365 days a year.

The system is registered with the Information Commissioner's Office.

The system will not record audio.

Recordings will have date and time stamps. This will be checked by the system manager termly and when the clocks change.

8. Storage of CCTV footage

Footage will be retained for 30 days. At the end of the retention period, the files will be overwritten automatically.

On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation.

Recordings will be downloaded and stored on a secure server, so that the data will remain secure and its integrity maintained, so that it can be used as evidence if required. Or held on a data device in a safe.

The Head of Estates will carry out periodic checks to determine whether footage is being stored accurately, and being deleted after the retention period.

9. Access to CCTV footage

Access must be sought from the DPO and will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log and complete Appendix B and return this to the DPO or the Head of Estates.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

9.1 Staff access

The following members of staff have authorisation to access the CCTV footage:

- The Principal
- The deputy principal
- The data protection officer
- The system manager
- Premises Teams
- Anyone with express permission of the DPO

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence, and may face disciplinary action.

9.2 Subject access requests (SAR)

According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

Upon receiving the SAR, the academy will immediately acknowledge the request and will then respond within 30 days during term time. The academy reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO in writing. When making a request, individuals should provide the academy with reasonable information such as the date, time and location the footage was taken to aid academy staff in locating the footage.

On occasion the academy will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation or as per DUAA guidelines.

Images that may identify other individuals need to be obscured to prevent unwarranted identification. The academy will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the academy will seek their consent before releasing the footage. If consent is not forthcoming then still images may be released instead, please refer to our Data Protection policy.

The academy reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

9.3 Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the Principal and the DPO.

The academy will comply with any court orders that grant access to the CCTV footage. The academy will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary.

The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the DPO.

10. Data protection impact assessment (DPIA)

The Trust follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including the replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

When the CCTV system is replaced, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate.

The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the Head of Estates and the DPO.

Those whose privacy is most likely to be affected, including the academy community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be put in place.

A new DPIA will be done whenever cameras are moved, or new cameras are installed.

If any security risks are identified in the course of the DPIA, the academy will address them as soon as possible.

11. Security

- The system manager will be responsible for overseeing the security of the CCTV system and footage
- The system will be checked for faults once a term
- Any faults in the system will be reported as soon as they are detected and repaired as soon as possible, according to the proper procedure
- Footage will be stored securely and encrypted wherever possible
- The CCTV footage will be password protected and any camera operation equipment will be securely locked away when not in use
- Proper cyber security measures will be put in place to protect the footage from cyber attacks
- Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

12. Complaints

Complaints should be directed to the Principal or the DPO and should be made according to the complaints policy.

13. Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes. The Chief Executive Officer is authorised to approve this policy on behalf of the Board of Directors.

14. Links to other policies

- Data protection policy
- Privacy notices for parents, pupils, staff, volunteers, visitors and suppliers
- Safeguarding policy

APPENDIX A: SUBJECT ACCESS REQUEST

Date of footage	
Start time of footage	
End time of footage	
Cameras of required footage	
Current time on recorder	
Time using speaking clock	
Person requesting footage	
Copy of footage has been recorded to USB	
Serial number of copied media disk	

The above information and associated CCTV footage has been compiled on behalf of:

The Park Federation Academy Trust

The footage detail above has been compiled in accordance with the Surveillance Camera Code of Practice. It is the recipient's responsibility to store and dispose of the recorded media in accordance with the code and the recipients take full responsibility for the safe keeping of the footage as detailed above. A copy of the codes can be obtained by visiting www.ico.gov.uk.

A £10.00 charge will be applied for producing information. The Park Federation Academy Trust will maintain a log of access requests detailing who the requests have been made by.

Issuer of the above footage

Name	Signature	Date

Recipient of the above footage

Name	Signature	Date
Address		
Identification		

APPENDIX B INTERNAL ACCESS REQUEST

CCTV – Request to view footage

In line with GDPR and our Policy this form should be completed prior to any footage being viewed

You should discuss your request with you Principal in the first instance, but **all** requests should be directed to Jas Sohal – Data Protection Officer and approval must be given before footage is viewed. The CCTV system has been installed to aid security of our buildings and boundaries as well as safe guarding of our staff and students and should not be used for personal use.

This section should be completed by the staff member who is requesting the CCTV should be viewed

Academy	Principal	Date of request (today's date)	Request made by (Print)	Signature

Description of Incident / Person(s)	**Camera Location:**	
Date of incident:	**Approximate time of incident (24 hours):**	
Why have you requested the CCTV be viewed?		

To be completed by Jas Sohal – Data Protection Officer

Requested approved	Signature/date/time	Request denied – reason given	Signature/date/time

To be completed by the Premises Team or the person viewing the CCTV

Name of person who recorded the image(s) onto digital media:	**Signature:**	**Date Recorded:**
Date images were recorded:	**Disc reference number/location of the footage:**	
Name of person who received the image(s):	**Signature:**	**Date:**

CCTV viewed at which location:			
Operated by:		**Position Held:**	
Record of down load taken by:		**Position Held:**	