

For the purposes of this policy, 'the Trust' refers to The Trust and all schools within the Trust.

CCTV Policy

Monitoring and review	
Author	Tanya Marley
Approver	Trustees
Owner	Tanya Marley, Director of Estates and Operations
Most recent review date:	May 2026
Date of next review	May 2027
Review frequency:	One Year
Category of policy	Statutory
Who has been consulted	
ADAPT or ADOPT	ADAPT

Version History Log

Version	Description of Change	Amended by	Date of Policy Release
1	Initial issue		1 September 2025
2	Adapted for Brookfields	CBE	October 2025
3	Annual review – Addition of second paragraph on Appendix C under the Data Storage Days heading	TMA	May 2026
3.1	Updated by Brookfields to V3	SMR	June 2026

CONTENTS:

1. Objectives	3
2. Purpose of This Policy	3
3. Public Information	4
4. Statement of Intent	4
5. System Management	5
6. Downloading Captured Data on to Other Media	5
7. Complaints About the Use of CCTV	6
8. Requests for Access by the Data Subject	6
<i>Appendix A: School CCTV System</i>	<i>7</i>
<i>Appendix B: Public Information</i>	<i>8</i>
<i>Appendix C: Data Storage Days, System Management and Requests for Access by Data Subject</i>	<i>9</i>

The Trust recognises that CCTV systems can be privacy intrusive.

For this reason, The Trust has carried out a **Data Protection Impact Assessment (DPIA)** with a view to evaluating whether the CCTV system in place is a necessary and proportionate means of achieving the legitimate objectives set out below.

The result of the data protection impact assessment has informed the Trust's use of CCTV and the contents of this policy.

The Trust is the Data Controller for the operation of CCTV. The Trust's Data Protection Officer DPO is

Data Protection Officer: Judicium Consulting Limited
Address: 5th Floor, 98 Theobalds Road
London
WC1X 8WB
Email: dataservices@judicium.com
Web: www.judiciumeducation.co.uk
Telephone: 0345 548 7000 (Option 1, then 1)

1. Objectives

Review of this policy shall be undertaken regularly and whenever new equipment is introduced, a review will be conducted, and a risk assessment put in place. We aim to conduct reviews no later than every two years.

The purpose of the CCTV system is to assist The Trust in achieving the following objectives:

- To protect pupils, staff and visitors against harm to their person and/or property
- To increase a sense of personal safety and reduce the fear of crime
- To protect The Trust buildings and assets
- To support the police in preventing, detecting and solving crime
- To assist in identifying, apprehending and prosecuting offenders
- To assist in establishing cause of accidents and other adverse incidents and prevent reoccurrence and
- To assist in managing The Trust

2. Purpose of This Policy

The purpose of this policy is to regulate the management, operation and use of the CCTV system (closed circuit television) at The Trust. The CCTV system used by The Trust comprises of ([See Appendix A](#))

3. Public Information ([See Appendix B](#))

4. Statement of Intent

CCTV cameras are installed in such a way that they are not hidden from view. We do not covertly record anyone. Signs are predominantly displayed where relevant so that staff, students, visitors and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

The CCTV system will seek to comply with the requirements both of the Data Protection Act and the most recent Commissioner's Code of Practice.

The Trust will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.

The system has been designed so far as possible to deny observation of adjacent private homes, gardens and other areas of private property.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.

Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police. Images will never be released to the media for purposes of entertainment.

The planning and design have endeavoured to ensure that the system will give maximum effectiveness and efficiency, 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, as required by the Code of Practice of the Information Commissioner, will be clearly visible on the site and make clear who is responsible for the equipment.

Where wireless communication takes place between cameras and a receiver, signals shall be encrypted to prevent interception.

CCTV images are not retained for longer than necessary, taking into account the purposes for which they are processed. Data storage is automatically overwritten by the system after a period of ([See Appendix C](#)) days.

Recorded images will only be retained long enough for any incident to come to light (e.g., for a theft to be noticed) and the incident to be investigated. In the absence of a compelling need to retain images for longer (such as an ongoing investigation or legal action), data will be retained for no longer than 6 months.

5. System Management ([See Appendix C](#))

6. Downloading Captured Data on to Other Media

In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings), any downloaded media used to record events from the hard drive must be prepared in accordance with the following procedures: -

- Each downloaded media must be identified by a unique mark.
- Before use, each downloaded media must be cleaned of any previous recording.
- The System Manager will register the date and time of downloaded media insertion, including its reference.
- Downloaded media required for evidential purposes must be sealed, witnessed and signed by the System Manager, then dated and stored in a separate secure evidence store. If a downloaded media 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 and signed by the System Manager, then dated and returned to the evidence store.
- If downloaded media is archived, the reference must be noted.
- If downloaded media is put onto a device, the device will be encrypted, and password protected.

Images may be viewed by the police for the prevention, detection and solving of crime and by the Systems Manager, his/her replacement and the Headteacher and other authorised senior leaders. However, where one of these people may be later called as a witness to an offence and where the data content may be used as evidence, it shall be preferable, if possible, for that person to withhold viewing of the data until asked to do so by the police.

A record will be maintained of the viewing or release of any downloaded media to the police or other authorised applicants.

Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the downloaded media (and any images contained thereon) remains the property of The Trust and downloaded media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The Trust also retain the right to refuse permission for the police to pass the downloaded media (and any images contained thereon) to any other person. On occasions when a Court requires the release of a downloaded media, this will be produced from the secure evidence store, complete in its sealed bag.

The police may require The Trust to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until needed by the police.

Applications received from outside bodies (e.g., solicitors or parents) to view or release images will be referred to The Trust's Data Protection Officer and a decision made by a senior leader of The Trust in consultation with The Trust's Data Protection Officer.

7. Complaints About the Use of CCTV

Any complaints in relation to The Trust's CCTV system should be addressed to the Headteacher of the relevant School.

8. Requests for Access by the Data Subject

The Data Protection Act provides data subjects – those whose image has been captured by the CCTV system and can be identified - with a right to access data held about themselves, including those obtained by CCTV. Requests for such data should be made to [\(See Appendix C\).](#)

Appendix A: School CCTV System

The school's CCTV system is implemented using Ubiquiti's UniFi Protect. The UniFi "Dream Machine" controller is secured in the IT server room and it manages the cameras around the school campus and contains the data storage device for video recordings. Access to this service is currently limited to the school network (or via VPN) only though it can be configured to use the UniFi Protect app via the internet if required.

A further UniFi Protect system is located at Pangbourne House and it manages two cameras for site security purposes. This system uses a UniFi Cloud Key with in-built storage for video recordings. Access to this system is possible via the UniFi Protect app when the Internet service is operational at Pangbourne House.

Appendix B: Public Information

Copies of this policy will be available to the public from The Trust office.

Camera Type	Location	Sound	Recording Capacity	Swivel/Fixed
G3 Flex	Pangbourne House Garden Exit	N	Y	Manual positioning only
G3 Dome	Pangbourne House Entrance Porch	N	Y	Manual positioning only
G3 Pro	Front of main school reception	N	Y	Manual positioning only
G3 Flex	Front of caretaker shed	N	Y	Manual positioning only
G3 Flex	IT Office (internal) facing outside	N	Y	Manual positioning only
G3 Flex	Library exterior wall	N	Y	Manual positioning only
G3 Flex	Old Staffroom (internal) facing exit to turning circle	N	Y	Manual positioning only
G3 Flex	Elliot's Building (PMLD Playground)	N	Y	Manual positioning only
G3 Flex	Primary School Entrance Lobby (internal)	N	Y	Manual positioning only
G3 Flex	Staff Workroom (internal) facing secondary playground	N	Y	Manual positioning only
G3 Flex	Secondary Playground Gate	N	Y	Manual positioning only
G3 Flex	IT Server room (internal)	N	Y	Manual positioning only

CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilets, changing facilities, etc.

Appendix C: Data Storage Days, System Management and Requests for Access by Data Subject

Data Storage Days

Data storage is automatically overwritten by the system after a period of 30 days.

CCTV footage will typically be retained for 30 days in line with the Trust's Data Retention Policy. However, where operational requirements justify a longer retention period (e.g. delays in incident discovery or investigation), footage may be retained for up to 60 days. Any extended retention period will be proportionate, documented and subject to regular review.

System Management

Access to the CCTV system and data shall be password protected and will be kept in a secure area.

The CCTV system will be administered and managed by the school IT Manager who will act as System Manager and take responsibility for restricting access, in accordance with the principles and objectives expressed in this policy. In the absence of the Systems Manager, the system will be managed by the Site Controller.

The system and the data collected will only be available to the Systems Manager, his/her replacement and appropriate members of the senior leadership team as determined by the Headteacher.

The CCTV system is designed to be in operation 24 hours each day, though The Trust does not guarantee that it will be working during these hours.

The System Manager will check and confirm the efficiency of the system regularly and in particular that the equipment is properly recording and that the cameras are functional.

Cameras have been selected and positioned so as to best achieve the objectives set out in this policy in particular by providing clear, usable images.

Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.

Where a person other than those mentioned above requests access to the CCTV data or system, the System Manager must satisfy him/herself of the identity and legitimacy of purpose of any person making such request. Where any doubt exists, access will be refused.

Details of all visits and visitors will be recorded in a system logbook including time/data of access and details of images viewed and the purpose for so doing.

Requests for Access by the Data Subject

Requests for such data should be made to the Headteacher