CCTV Policy

Approved by:	**Kate Green**	**Date: 05/05/2026**
Last reviewed on:	**May 2026**	
Next review due by:	**May 2027**	

Version History

Version	Approved By	Revision Date	Description of Change	Author
Version 1.0	Andrew Adams	May 2023	Initial Creation	Matt Rose
Version 2.0	Paul West	November 2024	Policy Re-write	Matthew Taylor & Andrew Adams
Version 2.1	Matthew Taylor	February 2025	Policy wording on External Viewers. Addition of: Emergency access to CCTV footage	Matthew Taylor
Version 2.2	Matthew Taylor	February 2025	Amended camera spec, and addition clarification for primary schools with no on-site IT support	Matthew Taylor
Version 2.3	Mathew Taylor	September 2025	Policy wording, making clearer to read and follow	Matthew Taylor
Version 2.4	Mathew Taylor	May 2026	Yearly Review	Matthew Taylor

Contents

1 Introduction

Spencer Academies Trust is committed to providing a safe and secure environment for all pupils, staff, and visitors. Closed Circuit Television (CCTV) plays an important role in supporting this commitment by helping to safeguard individuals, protect property, and ensure the effective management of our sites.

This policy sets out the standards and expectations for the use of CCTV across all academies and central offices within the Trust. Its purpose is to ensure that CCTV is used responsibly, lawfully, and transparently, balancing the benefits of enhanced security with the need to respect privacy and uphold data protection obligations.

The policy provides clear guidance on how CCTV systems must be installed, managed, and accessed. It outlines the responsibilities of authorised personnel, establishes protocols for footage handling, and ensures compliance with UK GDPR, safeguarding legislation, and best practice standards.

By following this policy, our academies and staff can be confident that CCTV is used consistently and appropriately to support safeguarding, protect assets, and maintain trust with our communities.

2 Policy Alignment and Governance

Policy Alignment

All decisions outlined in this policy align with relevant Trust and academy policies.

- SAT Safeguarding Policy
- SAT Acceptable Use Policy

This policy will also be guided by authoritative frameworks and guidance, including:

- ICO Guidance on CCTV
- Keeping Children Safe in Education

In cases of ambiguity, safeguarding considerations must take precedence when applying this policy.

Ongoing Review and Adaptation

Our Trust will regularly review and update its CCTV policy to reflect emerging risks, regulatory changes, and technological advancements.

We encourage feedback from students, colleagues, parents and carers for continuous improvement.

CCTV Hub

The CCTV Hub refers to the central SharePoint site used for the storage, management, and audit of all CCTV-related documentation and records:
https://spencertrust.sharepoint.com/sites/sat-CCTVHub

All references to the “site’s CCTV Hub” within this policy refer to this SharePoint location and its relevant site-specific folders.

Access to the CCTV Hub must be restricted to authorised personnel

3 CCTV Installation and System Requirements

All newly installed cameras must be selected from the approved kit list issued by Central I.T following the IT Procurement SOP.

Specification Requirements

Resolution

- **External cameras:** Minimum resolution of 8MP.
- **Internal cameras:** Minimum resolution of 4MP.

This ensures all footage is of sufficient quality for reliable monitoring and investigation.

Night Vision
All cameras must include night vision or low-light capability to ensure clear footage in low-light and no-light conditions.

Sound Recording
Cameras must be supplied without audio recording capability. Where this is not possible, audio functionality must be disabled prior to deployment and must not be used.

Standalone System
The CCTV system must operate as a standalone system and must not be integrated with access control, alarm systems, or other platforms.

Vape Detectors
CCTV cameras with integrated vape detection must not be installed unless explicitly approved by both the IT Director and the Data Protection Officer (DPO).

NVR and Storage

- All CCTV footage must be stored centrally on one or more Network Video Recorders (NVRs).
- Storage of footage directly on cameras is not permitted.
- Cloud storage must not be used unless explicitly approved by the IT Director.
- NVRs must retain a minimum of 30 days and a maximum of 90 days of footage. Where system capacity exceeds 90 days, automatic deletion must be enforced to ensure compliance.

Encryption

All CCTV systems must implement encryption both at rest and in transit to protect footage from unauthorised access and ensure compliance with UK GDPR.

Internet Access

CCTV systems must not have internet or remote access enabled by default unless explicitly approved by the IT Director and DPO. Where such functionality exists, it must be disabled by default.

4 Disclosure and External Viewers

External Viewers

CCTV footage, whether live or recorded, must not be disclosed to any individual or organisation outside the Trust. This explicitly includes parents and guardians.

Requests From Law Enforcement

Authorised law enforcement bodies (e.g. police) may request CCTV footage. These requests must be complied with and do not require a warrant. All disclosures must be logged in the site's CCTV Hub, and the Trust Data Protection Officer (DPO) must be notified.

Requests From Other Agencies

Requests from non-law enforcement organisations (e.g. local authorities, insurance companies) must not be fulfilled without a court order or appropriate legal authority.

Subject Access Requests (SARs)

Individuals have the right to request CCTV footage in which they are identifiable under UK GDPR and the Data Protection Act 2018. All such requests must be referred to the Trust Data Protection Officer (DPO) for review and approval prior to any disclosure.

Requests in Public Interest

CCTV footage relating to external areas (e.g. car parks or public-facing grounds) may be disclosed where there is a clear and justifiable public interest, such as road traffic incidents or medical emergencies. The School Principal may authorise such disclosures.

- Decisions must be limited to clearly defined public interest scenarios.
- All disclosures must be logged in the site's CCTV Hub.
- The Trust Data Protection Officer (DPO) must be informed at the earliest opportunity.

5 Access and Use of CCTV

Requests For Footage

All requests for CCTV footage must be formally recorded, reviewed, and approved prior to access.

Secondary and Central Sites

- All requests must be submitted via the ITS Helpdesk request form.
- Requests will be reviewed by authorised personnel for approval or rejection.
- Footage may only be accessed once approval has been granted.

Primary School Settings

- Requests must be recorded in a maintained CCTV log, stored on the site's CCTV Hub.
- The log must capture:
  - The requester
  - The approver
  - The reason for access
  - Date and time of access
- Requests must be reviewed and approved by authorised personnel prior to access.

Emergency Access to CCTV Footage

In urgent safeguarding or time-sensitive scenarios where waiting for approval may create risk, authorised personnel may access footage immediately.

A log entry must be completed straight after, recording:

- The individual who accessed the footage.
- The reason for immediate access.
- Details of the incident which require urgent review.

This ensures urgent matters are managed promptly while maintaining transparency and accountability.

Live View Access

CCTV is used for retrospective review and verification. Routine live monitoring is not permitted. Live access to CCTV systems is restricted and must not be used for general or unsupervised viewing.

Viewing Stations

A viewing station is a fixed, authorised display that provides a continuous live view from pre-defined CCTV camera(s). The cameras and views presented must be fixed and must not allow users to control, move, switch, or otherwise manipulate camera feeds. Viewing stations must not provide access to the wider CCTV system or recorded footage.

Live viewing stations may be permitted only where there is a clear safeguarding or operational requirement and must be approved in advance by the IT Director or the Data Protection Officer (DPO).

Viewing stations may be used for behaviour monitoring in appropriate public areas where there is no reasonable expectation of privacy, such as playgrounds, school halls/canteens, and external entry points.

Viewing stations must not be used in areas where there is a reasonable expectation of privacy, including classrooms, corridors, toilets, or changing areas.

Appropriate example: *Monitoring a playground or school hall/canteen to support behaviour management and safeguarding.*

Inappropriate example: *Monitoring a corridor to observe routine staff or pupil activity.*

All approved viewing stations must have a documented rationale outlining the safeguarding or operational need. This must be recorded and stored within the site's CCTV Hub, reviewed periodically to ensure continued appropriateness and available for audit upon request.

Authorised Personnel

CCTV Access Roles and Responsibilities

- Access to CCTV footage is strictly controlled and limited to authorised personnel only. Within the school, there are two defined user groups:
- CCTV Approvers: All CCTV footage requests must be formally reviewed and approved by a member of Senior Leadership Team before any footage is accessed.
- CCTV Reviewers: Selected members of staff, approved by Senior Leadership Team, are granted controlled access to the CCTV system. These users may review CCTV footage on behalf of the original requester once the request has been approved
- Each school must maintain an up-to-date list of authorised personnel, signed off by the School Principal.
- This list must be maintained through the ITS Helpdesk and can be authorised by the School Principal.

Automatic Authorised Roles

The following roles are automatically authorised to approve CCTV footage requests:

- SAT Executive Leadership Team
- SAT Central IT Leadership Team
- SAT Data Protection Officer
- SAT Central Facilities Team
- School Principal
- School Senior Leadership Team
- School Premises/Facilities Manager

Dual Authority Requirement

- Where the requester of footage is an authorised person, the request must be approved by a second authorised person before access is granted.
- The only exception is when the requester is the School Principal, who may access footage without secondary sign-off.

Restricted Authorised Personnel

- IT staff must not be designated as authorised personnel.
- Their role is limited to providing technical support, system maintenance, or facilitating access to footage when required.

Restricted Direct Access

- School Principals must not be given direct access to CCTV software.
- This measure ensures impartiality and avoids both conflicts of interest and any perception of bias.

6 Handling and Management of Footage

Playback and Downloads

- All playback views must be logged on the CCTV Request ticket, including the reason for access.
- If footage is downloaded, the log must include:
  - The individual who downloaded the footage.
  - The individual who requested the footage.
  - The reason for the download.
- Downloaded footage must only be stored within the site's CCTV Hub, where view-only access applies and automated retention and deletion policies are enforced.
- Where footage is required by an external agency, IT staff must facilitate the secure transfer.

Retention and Deletion of Footage

- CCTV footage must be retained for a minimum of 30 days and a maximum of 90 days, unless required for ongoing investigations or legal proceedings.
- After 90 days, all footage must be securely deleted in line with our trust's data retention policy and UK GDPR requirements.

Backup and Disaster Recovery

CCTV footage is not backed up due to its operational purpose and retention model. This is an accepted risk, balanced against data minimisation and storage limitations.

Exporting Footage

- When footage is exported for investigations or official purposes, it must be transferred securely, for example using encrypted USB drives or secure online transfer methods.

Incident Log Review

- All logs relating to access, playback, and downloads will be reviewed annually by the schools Senior Leadership Team (SLT).
- This review ensures compliance with policy requirements and relevant legislation.

7 Compliance and Safeguards

GDPR/Data Breach Protocols

- Any data breach involving CCTV footage must be reported immediately to the Data Protection Officer (DPO).
- A formal investigation will be undertaken to mitigate the breach and ensure compliance with GDPR reporting obligations.

Restricted Viewing Areas

- CCTV cameras must not be installed in areas where individuals have a reasonable expectation of privacy (e.g. changing rooms or other sensitive areas).
- Each site must maintain an up-to-date site map identifying all cameras and the areas covered.

CCTV Signage and Privacy Notices

- Clear signage must be displayed on all premises to inform individuals that CCTV surveillance is in operation.
- Signage must be positioned so that it is clearly visible immediately upon entry to the site and before individuals enter any monitored area. Where possible, this includes placement at all site entry points such as gates, fences, and vehicle or pedestrian access routes.
- In addition, signage must be displayed at all main entrances to buildings where CCTV is in operation, ensuring individuals are aware of monitoring as soon as they enter. Signage must include the purpose of monitoring and contact details, in line with UK GDPR.

User Training and Compliance

- All staff authorised to access CCTV systems must undertake regular training.
- Training must include legal obligations under UK GDPR, data protection requirements, and operational procedures for CCTV management.

8 Implementation and Support

CCTV Software Installation

Secondary Settings: CCTV monitoring or management software must only be installed on IT staff machines or fixed workstations (not portable) to ensure secure, audited access.

Primary and Special Settings: Where no full-time IT staff are present, CCTV software may be installed on up to two fixed workstations (not portable), excluding the School Principal's device.

Guidance and Contacts

For further guidance, questions, or concerns, please contact

Name	Role	Email
Andrew Adams	Data Protection Officer	AAdams@spencertrust.org.uk
Matthew Taylor	Director of Strategic IT & Infrastructure	MTaylor@spencertrust.org.uk