CCTV Policy

Author/owner: Trust Directors
Date adopted: September 2026
Anticipated review: September 2029

Our Vision

At The Three Saints Academy Trust, we believe every child deserves to learn, grow and flourish in a safe, nurturing and secure environment.

Our vision is underpinned by our Christian values and our commitment to ensuring that every child is protected from harm. The use of Closed-Circuit Television (CCTV) forms one element of our wider safeguarding, security and site management arrangements. It supports, but never replaces, the vigilance, professional judgement and care provided by our staff

1. Purpose

The purpose of this policy is to establish a consistent approach to the management, operation and use of CCTV systems across all schools and premises within The Three Saints Academy Trust.

This policy ensures that CCTV is operated:

- lawfully
- fairly
- proportionately
- transparently
- Securely
- in accordance with safeguarding responsibilities
- applicable with current UK legislation.

The Trust recognises that CCTV records personal data and therefore operates all surveillance systems in accordance with data protection legislation and the principles of necessity and proportionality, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability.

2. Scope

This policy applies to:

- All Schools within The Three Saints Academy Trust
- Central Trust Offices
- Pupils
- Employees
- Volunteers
- Governors & Directors
- Contractors

- Visitors
- External agencies accessing Trust premises.

The policy covers all CCTV systems owned or managed by the Trust.

This policy does not cover:

- body worn cameras
- dash cameras
- personal recording devices
- classroom recording used solely for teaching purposes.

Separate policies apply where appropriate.

3. Aims

The Trust operates CCTV to:

- safeguard children
- safeguard staff
- protect visitors
- deter criminal behaviour
- reduce vandalism
- protect Trust property
- support police investigations
- assist safeguarding investigations
- assist health and safety investigations
- assist behaviour investigations where appropriate
- provide evidence following serious incidents
- support emergency management.

The Trust will ensure that CCTV is never used in a way that is excessive or disproportionate.

4. Legislative Framework

This policy has been developed with reference to and will be interpreted alongside the following as applicable:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018

- Human Rights Act 1998
- Protection of Freedoms Act 2012
- Surveillance Camera Code of Practice
- Information Commissioner's Office (ICO) Guidance on Video Surveillance/CCTV
- Freedom of Information Act 2000
- Education Act 2002
- Working Together to Safeguard Children
- Keeping Children Safe in Education (KCSIE 2026)
- Health and Safety at Work Act 1974

The Trust will review this legislative framework when this policy is reviewed and sooner where significant legal or regulatory changes occur.

5. Data Protection Principles, Lawful Basis and Accountability

For every CCTV processing activity, the Trust will identify and document an appropriate lawful basis under Article 6 UK GDPR. The lawful basis selected must reflect the actual purpose and circumstances of the processing and will be recorded in the Trust's relevant privacy and records-of-processing documentation.

Where CCTV processing involves special category data or personal data relating to criminal convictions or offences, the Trust will identify and document any additional condition or legal requirement that applies under the UK GDPR and Data Protection Act 2018.

The Trust will ensure that CCTV processing is necessary and proportionate to the purpose for which it is used and will consider whether a less intrusive means could reasonably achieve the same outcome.

The Trust will maintain appropriate records to demonstrate compliance, including camera registers, DPIAs where required or mandated by this policy, access records, disclosure records, retention arrangements, incident records and relevant decisions.

- Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) will be completed before installing new CCTV or introducing a materially different surveillance capability, whenever the proposed processing is likely to result in a high risk to individuals. As a matter of Trust policy, the Trust will normally require a DPIA before:

- installing new cameras
- relocating cameras
- significantly changing camera coverage
- introducing audio recording

- introducing facial recognition, biometric identification, ANPR or other analytical surveillance
- introducing new surveillance technology that materially increases monitoring or intrusion

The DPIA will document the purpose, necessity, proportionality, lawful basis, risks to individuals, measures to mitigate those risks, retention, access, transparency and any residual risk.

6. Keeping Children Safe in Education (KCSIE)

The Trust recognises that safeguarding is everyone's responsibility.

In line with Keeping Children Safe in Education, CCTV forms one element of the Trust's wider safeguarding arrangements and may assist in:

- identifying safeguarding concerns
- investigating child protection incidents
- supporting multi-agency investigations
- protecting pupils from harm
- supporting safer recruitment investigations where appropriate
- protecting staff from false allegations
- assisting Designated Safeguarding Leads in establishing factual information.

CCTV does **not** replace:

- effective supervision
- staff vigilance
- safeguarding procedures
- professional curiosity
- timely reporting of concerns.

Where CCTV identifies a safeguarding concern, staff must immediately follow the Trust Child Protection and Safeguarding Policy.

The Designated Safeguarding Lead (DSL) will determine whether footage should be viewed as part of a safeguarding investigation.

7. Roles and Responsibilities

Board of Directors

The Board is responsible for:

- approving this policy

- ensuring legal compliance
- monitoring effectiveness
- ensuring appropriate governance.

Chief Executive Officer

The CEO has overall accountability for CCTV across the Trust.

They are responsible for:

- operational oversight
- ensuring consistency across Trust schools
- monitoring implementation
- ensuring policy compliance.

Headteachers

Headteachers are responsible for:

- ensuring local compliance
- maintaining camera registers
- authorising access to footage
- ensuring appropriate signage
- ensuring annual reviews.

Designated Safeguarding Leads

The DSL is responsible for:

- determining whether CCTV should be viewed for safeguarding purposes
- ensuring footage is handled securely
- working with external safeguarding agencies where appropriate.

Data Protection Officer

The DPO will:

- provide advice
- oversee GDPR compliance
- support Subject Access Requests
- advise on disclosures
- oversee DPIAs.

8. Camera Locations

Each school will maintain an up-to-date CCTV Register and will record as applicable, the camera number, location, purpose, area covered, audio capacity, retention period and DPIA status

Typical locations include:

- entrances
- exits
- reception areas
- playgrounds
- car parks
- external pathways
- perimeter fencing
- school halls
- shared circulation areas.

The exact location of cameras will be reviewed annually or following any significant changes or incidents.

9. Areas Where CCTV Will Not Normally Be Installed

The Trust recognises that individuals have a heightened expectation of privacy in certain locations.

Accordingly, CCTV will **not normally** be installed in:

- toilets
- changing rooms
- shower facilities
- medical rooms
- counselling rooms
- prayer or reflection spaces
- staff welfare areas.

Only in exceptional safeguarding circumstances will cameras be considered in or adjacent to such areas.

Any proposal must be supported by:

- a full Data Protection Impact Assessment
- safeguarding risk assessment

- advice from the Data Protection Officer
- approval by the CEO
- consultation with the School Committee or Board of Directors where appropriate
- consideration of parental communication where appropriate.

The Trust will always seek the least intrusive solution available and will document the reasons for any decisions.

11. Audio Recording

Audio recording is significantly more intrusive than visual recording and will be disabled by default unless a specific, documented need has been established.

Continuous audio recording will not be used unless the Trust can demonstrate a compelling and lawful justification, necessity and proportionality. Any proposed audio recording must be considered through the DPIA process and approved by the DPO and an appropriate senior officer.

Where audio is recorded, signage and privacy information must clearly state that audio is captured, the purpose, lawful basis and relevant contact information. Audio must not be enabled merely because equipment has that capability.

12. Signage and Privacy Information

Appropriate CCTV signs must be displayed before individuals enter areas in which they are likely to be recorded. Signs must be clear, visible and appropriate to the location.

At a minimum, the first-layer information should identify that CCTV/surveillance is in operation, the purpose(s), the Trust or relevant controller identity and an appropriate contact route. The sign must direct individuals to the Trust's fuller privacy information.

The Trust's privacy notice will explain, as applicable, purposes, lawful basis, categories of personal data, retention, recipients/disclosures, rights, contact details for the Trust and DPO, and how concerns may be raised with the ICO.

Where audio or materially different surveillance technology is used, the first-layer information will be adapted to make the additional processing clear.

13. Operation, Monitoring and Viewing

CCTV will only be monitored or viewed by authorised personnel with a legitimate need to do so. Access will be role-based and limited to the minimum necessary.

Operators must not use CCTV for personal curiosity, monitoring unrelated to the stated purpose, harassment, discrimination or any other unauthorised purpose.

Viewing must be proportionate to the reason for access. Where practical, live monitoring will be avoided unless necessary for the stated purpose.

Every access to stored footage must be recorded in the CCTV Access Log, including the date, time, person accessing, reason, cameras/footage viewed, incident reference where applicable and authorisation.

14. Retention and Secure Disposal

There is no single statutory CCTV retention period applicable to all Trust systems. The Trust will retain footage for the shortest period reasonably necessary for the purpose for which it is processed.

Each camera/system will have a documented retention period in the CCTV Register. The chosen period must be justified by operational need and reviewed regularly.

Where footage is required for an identified safeguarding, disciplinary, complaint, legal, insurance or criminal investigation, the relevant footage may be preserved for as long as necessary for that matter. The reason for extended retention must be documented and access restricted.

Routine footage that is no longer required must be securely and automatically deleted or overwritten wherever technically possible.

CCTV access logs will be retained in accordance with the Trust's records retention schedule and for no longer than necessary to demonstrate accountability, investigate misuse and meet applicable legal or governance requirements. Six years is not to be treated as a universal statutory CCTV retention requirement.

15. Security and Technical Controls

unique user accounts where technically possible

strong passwords and appropriate authentication

role-based access

restricted remote access

secure networks and systems

regular review of user permissions

audit logging where available

secure export and transfer of footage

appropriate physical security of recording equipment

prompt removal of access when staff leave or no longer require it

Where a third-party provider processes CCTV personal data on behalf of the Trust, the Trust will ensure appropriate contractual arrangements and processor requirements are in place.

16. Disclosure to Police and Other Agencies

Footage may be disclosed to police, safeguarding partners, courts, insurers, legal advisers or other agencies where there is a lawful basis and the disclosure is necessary and proportionate.

Requests and disclosures must be documented, including the requester, authority/identity where appropriate, date, footage released, purpose, method of transfer and authorising officer.

Footage must be transferred securely. The Trust will not disclose footage merely because a third party asks for it; the legal basis and necessity of the disclosure must be considered.

17. Subject Access Requests and Other Rights

Individuals may exercise applicable data protection rights in relation to CCTV. The Trust will maintain a procedure for identifying relevant footage, locating it, assessing third-party privacy, applying lawful redaction or masking where appropriate, and responding within the applicable statutory period.

A request from a parent or carer does not automatically entitle that person to receive unrestricted footage of other pupils or individuals. Requests involving children will be handled in accordance with data protection law, the child's circumstances, parental responsibility, the child's expectations and rights, and the rights of other individuals captured.

Where footage is relevant to a legal, safeguarding, disciplinary or criminal matter, the Trust will take appropriate steps to preserve it while the matter is ongoing.

18. Safeguarding, Behaviour and Staff Investigations

CCTV may be used where necessary and proportionate to establish factual information in safeguarding, serious behaviour, health and safety, disciplinary or related investigations. CCTV must not be used as a substitute for fair investigation procedures or professional judgement.

Access will be limited to those who need the footage for the relevant investigation. Decisions to use footage in employment or pupil disciplinary processes must comply with applicable Trust policies and procedural fairness.

19. Intrusive or Emerging Surveillance Technologies

Facial recognition, biometric identification, ANPR, behavioural analytics, automated detection or other materially intrusive surveillance technology must not be introduced without prior legal/data protection assessment and approval.

Where biometric data is processed for uniquely identifying an individual, the Trust must satisfy the applicable Article 6 and Article 9 requirements and any additional requirements under the Data Protection Act 2018. A DPIA will be mandatory under this policy.

The Trust will not assume that technology is lawful merely because it is technically available.

20. Complaints, Breaches and Incidents

Complaints concerning CCTV will be handled under the Trust complaints procedure and, where relevant, the data protection complaints procedure.

Any suspected loss, unauthorised access, accidental disclosure, cyber incident or other CCTV data breach must be reported promptly to the DPO or designated information governance contact and managed under the Trust Data Breach Procedure.

The Trust will assess whether notification to the ICO or affected individuals is required.

21. Freedom of Information

Where the Trust is subject to the Freedom of Information Act 2000, requests involving CCTV or related records will be handled under the Trust's FOI procedure. Data protection rights and FOI obligations will be considered separately and the appropriate regime applied.

22. Equality and Human Rights

The Trust will consider equality, privacy and human rights impacts when introducing or reviewing CCTV. Surveillance must not be operated in a discriminatory, excessive or unjustifiably intrusive manner.

23. Annual Compliance Review

Each school will complete an annual CCTV compliance audit covering governance, lawful basis, DPIAs, signage, camera necessity, privacy, security, access, disclosures, retention, equipment and rights requests.

The Trust will review this policy at least annually and sooner where there are material changes in law, ICO guidance, safeguarding guidance, technology or Trust arrangements.

24. Key Compliance Records

- CCTV Camera Register
- DPIAs and related assessments
- CCTV Access Logs
- Police/External Disclosure Logs
- Retention and deletion records
- CCTV privacy notices and signage checks
- Subject Access Request records
- Data breach/incident records
- Annual CCTV Compliance Audit
- Records of decisions concerning intrusive technologies

APPENDIX A
CCTV Camera Register (School Template)
Three Saints Academy Trust
School: _____
Academic Year: _____
Date Reviewed: _____

Camera No.	Location	Purpose	Area Covered	Audio Recording (Y/N)	Fixed/PTZ	Retention Period	DPIA Required?	Notes
1								
2								
3								
4								
5								
6								
7								
8								

Declaration
I confirm that all CCTV cameras have been reviewed and remain necessary, proportionate and compliant with the Trust CCTV Policy.
Headteacher:
Name: _____
Signature: _____
Date: _____

APPENDIX B
Annual CCTV Compliance Audit
Three Saints Academy Trust
School: _____
Audit Date: _____
Completed by: _____

Governance

Question	Yes	No Action Required
CCTV Policy reviewed within previous 12 months	☐	☐
Camera Register updated	☐	☐
DPIA completed where required	☐	☐
Local Governing Body informed of significant changes	☐	☐

Signage

Question	Yes	No	Action Required
Signs visible at entrances	☐	☐	
Signs comply with ICO guidance	☐	☐	
Contact details displayed	☐	☐	

Camera Locations

Question	Yes	No	Action Required
Cameras remain necessary	☐	☐	
No unnecessary intrusion into neighbouring properties	☐	☐	
No inappropriate coverage of private areas	☐	☐	

Data Protection

Question	Yes	No	Action Required
Passwords secure	☐	☐	
Access restricted	☐	☐	
Access logs maintained	☐	☐	
Police disclosures recorded	☐	☐	
SAR process understood	☐	☐	

Equipment

Question	Yes	No	Action Required
Cameras operational	☐	☐	
Time/date correct	☐	☐	
Image quality acceptable	☐	☐	
Recording functioning	☐	☐	
Maintenance completed	☐	☐	

Summary of Actions

Headteacher Signature:

Date:

APPENDIX C
CCTV Access Log
Three Saints Academy Trust

Date Time	Name	Job Title	Reason for Access	Cameras Viewed	Incident Reference	Authorised By	Signature

Notes
Every access to CCTV footage must be recorded.
Only authorised personnel may access footage.
Logs should be retained for six years.

APPENDIX D
Police Disclosure Log
Three Saints Academy Trust

Date	Police Force	Officer Name	Collar Number	Incident/Crime Ref	Footage Released	Method of Transfer	Authorised By	Date Returned/Destroyd

---

Declaration
I confirm the footage has been released in accordance with the Trust CCTV Policy and UK GDPR.
Authorising Officer:

Position:

Date:

APPENDIX E
CCTV Subject Access Request Form
Three Saints Academy Trust
Applicant Details
Name

Address

Telephone

Email

Identity Verification

☐ Passport

☐ Driving Licence

☐ Birth Certificate

☐ Other

Details

Details of Requested Footage

School

Location

Date

Approximate Time

Description of Incident

Declaration

I understand that:

- I am requesting access to my personal data.
- Identification will be required.
- Images of third parties may be redacted.
- The Trust may refuse disclosure where exemptions apply under UK GDPR or safeguarding legislation.

Signature

Date

Office Use Only

Request Received

Verified By

Reference Number

Response Due By

Outcome

☐ Granted

☐ Partially Granted

☐ Refused

Reason

Legal Review Note

This policy is intended to support compliance but does not itself establish compliance for every individual CCTV installation. Each school/system must be operated consistently with its documented purposes, lawful basis, DPIA where required, privacy information, camera register, retention arrangements, security controls and applicable law.

This revised draft has been prepared against current ICO CCTV guidance and current UK Government information available in August 2026. It should be reviewed by the Trust's DPO and, where appropriate, specialist education/data protection legal advisers before formal adoption.

APPENDIX F

CCTV Data Protection Impact Assessment (DPIA) Checklist

To be completed before installing new cameras or making significant changes to CCTV coverage.

School

Date

Completed By

Purpose

Why is CCTV required?

☐ Safeguarding

☐ Crime Prevention

☐ Health & Safety

☐ Site Security

☐ Vandalism

☐ Other

Necessity

Have alternative measures been considered?

☐ Yes

☐ No

Details

Proportionality

Is CCTV proportionate to the identified risk?

☐ Yes

☐ No

Evidence

Privacy Assessment

Does the camera overlook:

Area	Yes	No
Public Highway	☐	☐
Neighbouring Property	☐	☐
Residential Garden	☐	☐
Staff Welfare Area	☐	☐
Toilets	☐	☐
Medical Room	☐	☐
Changing Room	☐	☐

If Yes, explain mitigating actions.

Data Security

Requirement	Yes	No
Password Protected	☐	☐
Encryption Used	☐	☐
Access Restricted	☐	☐
Retention Period Appropriate	☐	☐
Automatic Deletion Enabled	☐	☐

Consultation

Have the following been consulted where appropriate?

Stakeholder	Yes	No
Headteacher	☐	☐
CEO/Deputy CEO	☐	☐
Data Protection Officer	☐	☐
DSL	☐	☐
ICT Provider	☐	☐
Governors	☐	☐

Risk Assessment

Risk	Likelihood	Impact	Mitigation
Privacy intrusion			
Data breach			
Equipment failure			
Misuse of footage			
Inappropriate disclosure			

Final Decision

☐ Approved

☐ Approved with Conditions

☐ Not Approved

Reason

_____

_____

_____

Authorisation

Headteacher

Name: _____

Signature: _____

Date: _____

Data Protection Officer

Name: _____

Signature: _____

Date: _____