

Three Counties Academy Trust



Surveillance and CCTV Policy

#FI21

Last amended 30th September 2026 (v1.0)

Policy lifespan: 3 years. Subject to annual compliance check. Next full review 29th September 2029.

Version history

Date	Version	Details	Actioned by	PDF to Websites	Word to Governor Hub
30.09.26	1.0	Formatted to house style and checked against model for updates	MF	✓	✓

Contents:

Version history

Policy abbreviations and acronyms

Statement of intent

Member, Trustee, Local Governor and Staff Summary

Parent and Visitor Summary

1. Legal framework
2. Definitions
3. Roles and responsibilities
4. Purpose, justification and transparency
5. Data protection
6. Protocols
7. Security
8. Code of practice
9. Access
10. Use of automatic number-plate recognition (ANPR)

Monitoring and review

Trust Glossary

Policy abbreviations and acronyms

ANPR	Automated Number Plate Recognition
CCTV	Closed-Circuit Television
CFO	Chief Financial Officer
CPS	Crown Prosecution Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
FRT	Facial Recognition Technology
ICO	Information Commissioner's Office
LIA	Legitimate Interests Assessment
SAR	Subject Access Request
TCAT	Three Counties Academy Trust
UK GDPR	UK General Data Protection Regulation

NB. Where the term “parent” or “parents” is used this includes those who act as carers or have parental responsibility.

NB. Staff roles noted within this policy may also include those staff performing that role in an ‘Acting’ capacity.

Statement of intent

Three Counties Academy Trust (TCAT) is committed to providing safe, secure and appropriately protected environments for pupils, staff, visitors and others using its premises. As part of the measures used to support safeguarding, site security and the prevention and investigation of incidents, TCAT may operate closed-circuit television (CCTV) and other appropriate surveillance systems across its schools and premises.

TCAT recognises that the use of surveillance technology involves the processing of personal data and has the potential to affect an individual's privacy. Surveillance will therefore only be used where there is a clear and legitimate purpose and where its use is considered necessary, proportionate and appropriate to the circumstances. TCAT will seek to balance the benefits of surveillance against the rights and reasonable expectations of privacy of pupils, staff, visitors and other individuals.

The purpose of this policy is to establish a clear framework for the operation and management of CCTV and surveillance systems across TCAT and to ensure that personal data obtained through these systems is collected, used, stored, accessed, disclosed and deleted appropriately and in accordance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

TCAT will ensure, as far as reasonably practicable, that surveillance systems are appropriately located and configured; that individuals are informed when surveillance is taking place; that recorded images are of sufficient quality for their intended purpose; and that access to recordings is restricted to authorised individuals. Recordings will be retained only for as long as there is a legitimate reason for doing so and will be protected against unauthorised access, disclosure, alteration or loss.

CCTV and surveillance systems may be used for legitimate purposes including:

- Supporting the maintenance of a safe and secure environment
- Supporting the safeguarding and welfare of pupils, staff and visitors
- Protecting Trust property, buildings, equipment and other assets
- Deterring, detecting and assisting in the investigation of criminal activity, antisocial behaviour, vandalism and other incidents
- Supporting the investigation of significant breaches of Trust or school policies where the use of surveillance footage is necessary and proportionate
- Providing evidence in relation to incidents, complaints, disciplinary matters or other legitimate investigations
- Assisting the police, emergency services, safeguarding agencies or other authorised bodies where disclosure is lawful and appropriate

Surveillance will not be used for purposes incompatible with those for which it was introduced, nor will it be used in a manner that is excessive or unjustifiably intrusive. Particular consideration will be given to the location of cameras and the reasonable expectation of privacy associated with different areas of Trust premises.

Through this policy, TCAT seeks to ensure that its use of CCTV and surveillance contributes positively to the safety and security of its school communities while maintaining appropriate safeguards for the privacy and data protection rights of individuals.

Member, Trustee, Local Governor and Staff Summary

Strategic oversight

- Ensure surveillance and CCTV systems are only used where there is a clear, legitimate and proportionate need linked to safeguarding, security, welfare or the investigation of incidents
- Maintain confidence that TCAT balances safety and security with individuals' rights to privacy and data protection
- Recognise that the Trust Board has overall responsibility for ensuring surveillance records, security arrangements and access controls comply with legal requirements
- Receive assurance that surveillance systems are regularly reviewed, justified and remain compliant with current legislation and guidance
- Ensure appropriate governance is in place for any future use of biometric technologies or ANPR systems, including completion of Data Protection Impact Assessments (DPIAs) before implementation

Compliance and data protection

- CCTV footage is personal data and must be managed in accordance with UK GDPR, the Data Protection Act 2018 and related legislation
- TCAT must undertake DPIAs before installing surveillance, CCTV or biometric systems and address any identified risks
- Surveillance systems must be transparent, appropriately signposted and used only for their intended purposes
- Access to footage must be tightly controlled and restricted to authorised personnel only

Assurance expectations

- CCTV must not be installed within classrooms or changing facilities and must not be used in an excessive or intrusive manner
- Audio recording and facial recognition technology are generally prohibited unless strict legal, operational and proportionality requirements can be demonstrated
- CCTV should be retained only for as long as necessary and securely protected from unauthorised access, disclosure or misuse

Why CCTV is used

- To help maintain safe and secure school environments for pupils, staff and visitors

- To support safeguarding and welfare arrangements
- To help prevent, deter and investigate criminal activity, vandalism, antisocial behaviour and significant policy breaches
- To provide evidence when investigating incidents, complaints, disciplinary matters or safeguarding concerns where appropriate

Staff responsibilities

- Follow all TCAT procedures relating to access, use, disclosure and protection of CCTV footage
- Ensure CCTV information is treated as confidential personal data and only accessed where authorised and necessary
- Complete relevant training and understand data protection responsibilities before accessing CCTV systems or recordings
- Report concerns about data protection, misuse of recordings or system security through appropriate management channels

What staff should expect

- CCTV operation will be clearly communicated through signage and other notifications
- CCTV will not be used for routine staff monitoring or unjustified surveillance of individuals
- Covert surveillance is not permitted for monitoring staff and would only be considered in exceptional circumstances where legally justified
- Individuals retain rights relating to access to their personal data, including CCTV recordings, through TCAT's Subject Access Request procedures

What Good Practice Looks Like

- Surveillance is necessary, proportionate and regularly reviewed
- Privacy is respected alongside safeguarding and security needs
- Access to footage is limited and auditable
- CCTV data is securely stored and deleted when no longer required
- Staff understand their responsibilities and receive appropriate training
- Governance arrangements provide effective oversight and challenge of surveillance activities

Parent and Visitor Summary

Purpose

This policy explains how TCAT helps keep schools safe and secure through the appropriate use of CCTV and surveillance systems, while protecting the privacy and rights of pupils, parents, visitors and staff.

What CCTV is used for

TCAT schools may use CCTV to:

- Help safeguard pupils, staff and visitors
- Improve site security and help prevent crime, vandalism and antisocial behaviour
- Support investigations into incidents, complaints or serious breaches of school rules
- Assist emergency services, safeguarding agencies and the police where appropriate and lawful
- Protect school buildings, equipment and other property

How privacy is protected

- CCTV is only used where there is a clear and legitimate need
- Cameras are positioned carefully to avoid being unnecessarily intrusive
- CCTV is not used in changing facilities and is not intended for routine monitoring of individuals
- Clear signs are displayed where CCTV is in operation
- TCAT aims to balance safety and security with everyone's right to privacy

How recordings are managed

- CCTV footage is treated as personal data and managed in line with data protection law
- Access to recordings is restricted to authorised staff only
- Recordings are stored securely and protected against unauthorised access
- Footage is only kept for as long as there is a legitimate reason to retain it and is then securely deleted

- Footage may be shared with the police or other authorised agencies where legally required or appropriate

Biometric and facial recognition systems

- TCAT does not use live facial recognition technology as part of our CCTV systems
- Any future use of biometric technologies would require careful assessment, compliance with legal requirements and appropriate safeguards
- Pupils' rights and parental rights relating to biometric data are protected by law and TCAT procedures

Your rights

- Individuals have rights under data protection legislation regarding personal data captured by CCTV
- Requests for access, correction, restriction or deletion of personal data will be considered in accordance with data protection legislation and TCAT policies

Key Message

TCAT uses CCTV to help create a safer environment for pupils, staff, parents and visitors. Systems are operated transparently, used only for legitimate purposes, and supported by strict security and data protection controls to ensure privacy rights are respected at all times.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- [Regulation of Investigatory Powers Act 2000](#)
- [Protection of Freedoms Act 2012](#)
- [The UK General Data Protection Regulation \(GDPR\)](#)
- [Data Protection Act 2018](#)
- [Freedom of Information Act 2000](#)
- [Human Rights Act 1998](#)
- [The Education \(Pupil Information\) \(England\) Regulations 2005 \(as amended in 2016\)](#)
- [The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#)
- [School Standards and Framework Act 1998](#)
- [Children Act 1989](#)
- [Children Act 2004](#)
- [Equality Act 2010](#)
- [Home Office 'The Surveillance Camera Code of Practice'](#)
- [ICO 'Guide to the UK General Data Protection Regulation \(UK GDPR\)'](#)
- [ICO 'CCTV and video Surveillance'](#)
- [Biometrics and Surveillance Camera Commissioner 'Surveillance Camera Code of Practice' data of children in schools and colleges](#)
- [Herefordshire Council 'Schools: CCTV Guidance Note'](#)
- [DfE 'Data protection in schools'](#)

Where legislation has been passed or updated during the shelf life of this policy, we will always apply the latest version available irrespective of the version quoted here.

This policy operates in conjunction with the following policies:

- Subject Access Request (SAR) Policy (FI9)

- Freedom of Information Policy (FI10)
- Data Protection Policy (FI20)
- Statement on the Processing of Biometric Data (GN17)
- Photography and Images Policy (SG9)
- Trust and School Security Policy (SG34)
- Online Safety Policy (SG43)
- Privacy Statements (FI12(A through J))

Central TCAT policies have the policy number identified, e.g. "SG1". Where no policy number is identified this indicates the policy is a school specific policy available from an individual TCAT school's website.

2. Definitions

For the purpose of this policy the following definitions are given for the below terms:

- **Surveillance** – monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable
- **Overt surveillance** – Surveillance which is clearly visible and signposted around any TCAT school and does not fall under the Regulation of Investigatory Powers Act 2000
- **Covert surveillance** – any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects will not be informed of such surveillance

TCAT does not condone the use of covert surveillance when monitoring TCAT staff, pupils and/or volunteers. Covert surveillance will only be operable in extreme circumstances.

- **Biometric data** – data which is related to the physiological characteristics of a person, which confirm the unique identification of that person, such as fingerprint recognition, facial recognition (FRT), or iris recognition
- **Automated biometric recognition system** – a system which uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically'

- **Facial recognition** – the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template

3. Roles and responsibilities

The role of the DPO and where appropriate the CFO includes:

- Dealing with freedom of information requests and subject access requests (SARs) in line with legislation, including the Freedom of Information Act 2000
- Ensuring that as a data controller, TCAT handle and process surveillance and CCTV footage in accordance with data protection legislation
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements
- Considering the appropriate lawful basis to use to legitimise CCTV use
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period
- Advising on whether the use of CCTV is appropriate and proportionate for TCAT's circumstances
- Advising on where to place security cameras
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request
- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by TCAT or our schools, their rights for the data to be destroyed and the measures implemented by TCAT and our schools to protect individuals' personal information
- Preparing reports and management information on TCAT and our schools level of risk related to data protection and processing performance
- Reporting to the highest management level of the Trust, e.g. the Trust Board
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role
- Monitoring the performance of TCATs data protection impact assessment (DPIA) and providing advice where requested
- Presenting reports regarding data processing at TCAT and our schools to Executive Leaders and the Trust Board

TCAT, as the corporate body, is the data controller. The Trust Board therefore has overall responsibility for ensuring that records are maintained, including security and access arrangements in accordance with regulations.

The Chief Finance Officer deals with the day-to-day matters relating to data protection and thus, for the benefit of this policy will act as the data controller.

The role of the data controller includes:

- Processing surveillance and CCTV footage legally and fairly
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure – especially when processing over networks
- Ensuring that the processing of any biometric data, including any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and Protection of Freedoms Act 2012
- Identifying the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented
- Ensuring that the processing of biometric data is done so in line with the TCATs Statement on the Processing of Biometric Data and the Data Protection Policy
- Monitoring legislation to ensure TCAT is using surveillance fairly and lawfully
- Reviewing the Surveillance and CCTV Policy to ensure it is compliant with current legislation
- Communicating any changes to legislation with the Trust Board

The role of Executive Headteacher, Headteacher and where delegated Head of School includes:

- Meeting with the CFO and DPO to decide where CCTV is needed to justify its means
- Conferring with the CFO and DPO with regard to the lawful processing of the surveillance and CCTV footage
- Monitoring legislation to ensure their school is using surveillance fairly and lawfully
- Communicating any changes to legislation with all members of their staff

4. Purpose, justification and transparency

TCAT will only use surveillance cameras for the safety and security of our schools, staff, pupils and visitors. This may include, but is not limited to:

- Assisting in emergency situations
- Managing lockdowns
- Supporting the application of internal policies
- Supporting the safeguarding of pupils
- Providing a sense of security for pupils and staff

TCAT will consider which lawful basis is most appropriate to use. This will be either public task or legitimate interests.

When using legitimate interests as its lawful basis, TCAT will complete a legitimate interests assessment.

Consent will not be appropriate as the lawful basis for TCAT's use of CCTV due to the unlikelihood of being able to obtain consent from everyone who may be captured on CCTV, and because it is difficult for people to opt out.

In deciding whether CCTV is appropriate, TCAT will consider why it is necessary and appropriate.

TCAT will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in school classrooms or any changing facility. Where historic CCTV hardware exists within classrooms these will not be monitored, or footage used and will be decommissioned at an appropriate time.

If the surveillance and CCTV systems fulfil their purpose and are no longer required, or it is deemed such systems cannot be justified, TCAT will deactivate them and explore less intrusive alternatives.

In our use of surveillance and CCTV, TCAT will be open and honest towards the TCAT community. TCAT will consult with pupils, parents and staff, explain where the cameras will be, and explain what the footage will be used for.

Clearly visible signs will also be in place to inform people that CCTV is in use.

5. Data protection

Data collected from surveillance and CCTV will be:

- Processed lawfully, as determined by a DPIA, or from advice from the DPO. In less common circumstances, lawful processing will be determined by a legitimate interests assessment (LIA)
- Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people
- Processed in a transparent manner, meaning that people are informed when their data is being captured
- Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
 - Further processing for archiving data in the public interest
 - Scientific or historical research
 - Statistical purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The use of surveillance cameras, CCTV, and biometric systems, will be critically analysed using a DPIA, in consultation with the DPO.

A DPIA will be carried out prior to the installation of any surveillance, CCTV, or biometric system. A DPIA will:

- Describe the nature, scope, context, and purposes of the processing
- Assess necessity, proportionality, and compliance measures
- Identify and assess risks to individuals

- Identify any additional measures to mitigate those risks

Sensitive data obtained via biometric technology will be processed via special conditions (listed in Article 9 of the UK GDPR).

If the DPIA reveals any potential security risks or other data protection issues, TCAT will ensure they have provisions in place to overcome these issues.

Where TCAT identifies a high risk to an individual's interests, and it cannot be overcome, TCAT will consult the ICO before they use CCTV, and will act on the ICO's advice.

While data protection laws do not prescribe any specific minimum or maximum retention periods for CCTV footage, TCAT will not routinely hold on to footage longer than is necessary. CCTV footage will ordinarily be deleted after 30 days. Footage may be held for longer in exceptional circumstances, e.g. if it is required to assist a criminal investigation.

TCAT will not use CCTV with live-facial recognition technology as this is unlikely to be justifiable. If the system chosen by TCAT does contain this feature, it will be switched off by default to ensure biometric data is not unnecessarily processed.

CCTV will not be routinely used to record conversations or otherwise act as an overly intrusive means of security. Any system that has the capability to record audio will have this feature switched off unless an identified need has been met as identified as set out in section 7 of this policy.

6. Protocols

The surveillance system will be registered with the ICO in line with data protection legislation.

The surveillance system is a closed digital system.

Warning signs have been placed throughout the premises where the surveillance system is active, as mandated by the ICO's Code of Practice. Warning signs will be more prominent in areas where surveillance is less expected to be in operation, and when using systems that can capture a large amount of personal data at one time.

The surveillance system has been designed for maximum effectiveness and efficiency; however, TCAT cannot guarantee that every incident will be detected or covered and 'blind spots' may exist.

The surveillance system will not be used to focus on a particular group or individual unless an immediate response to an incident is required.

The surveillance system will not be trained on private vehicles or property outside the perimeter of any TCAT school.

FRT will be justifiable, proportionate, and able to address specific needs.

7. Security

Access to the surveillance system, software and data will be strictly limited to authorised operators, and will be password protected, and where appropriate, will be encrypted.

In exceptional cases where large amounts of information need to be collected and retained, TCAT will consider using cloud storage. This will be secure and only accessible to authorised individuals.

The main control facility is kept secure and locked when not in use.

If, in exceptional circumstances, covert surveillance is planned, or has taken place, copies of the Home Office's [authorisation forms](#) will be completed and retained.

Surveillance and CCTV systems will be tested for security flaws at regular intervals to ensure that they are being properly maintained at all times.

The DPO, CFO and Executive Headteacher/Headteacher or where delegated, Head of School will decide when to record footage.

Staff will be trained in security procedures, and sanctions will be put in place for those who misuse security system information. Staff will be made aware that they could be committing a criminal offence if they do this.

The ability to produce copies of information will be limited to the appropriate staff.

Any unnecessary footage captured will be securely deleted from the TCAT and school systems.

Each system will have a separate audio and visual system that can be run independently of one another. TCAT will not record audio unless it has:

- Identified a particular need or issue and can evidence that this need must be addressed by audio recording
- Considered other less privacy intrusive methods of achieving this need
- Reviewed the other less privacy intrusive methods and concluded that these will not appropriately address the identified issue and the only way to do so is via the use of audio recording

Any cameras that present faults will be repaired immediately as to avoid any risk of a data breach.

Visual display monitors are located in secure areas.

8. Code of practice

TCAT understands that recording images of identifiable individuals constitutes as processing personal information, so it is done in line with data protection principles.

TCAT notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, signs, letters and emails.

CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.

All surveillance footage will be kept for 30 days for security purposes, which may only be exceeded to assist with a criminal investigation; the Headteacher/Head of School and the Chief Finance Officer are responsible for keeping the records secure and allowing access.

TCAT schools have a surveillance system for the purpose of the prevention and detection of crime and the promotion of the health, safety and welfare of staff, pupils and visitors.

The surveillance and CCTV system is owned by TCAT and images from the system are strictly controlled and monitored by authorised personnel only.

TCAT and our schools will ensure that the surveillance and CCTV systems are used to create a safer environment for staff, pupils and visitors to our schools, and to ensure that its operation is consistent with the obligations outlined in data protection legislation.

The surveillance and CCTV system will:

- Be designed to take into account its effect on individuals and their privacy and personal data
- Be transparent and include a contact point which enables people to request information and submit complaints via the DPO
- Have clear responsibility and accountability procedures for images and information collected, held and used
- Have defined policies and procedures in place which are communicated throughout TCAT and our schools
- Only keep images and information for as long as required
- Restrict access to retained images and information with clear rules on who can gain access
- Consider all operational, technical and competency standards, relevant to the surveillance and CCTV system and its purpose, and work to meet and maintain those standards in accordance with the law
- Be subject to stringent security measures to safeguard against unauthorised access
- Be regularly reviewed and audited to ensure that policies and standards are maintained
- Only be used for the purposes for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement
- Be accurate and well maintained to ensure information is up to date

To comply with the requirements of the Protection of Freedoms Act 2012, TCAT and our schools will notify all parents of its intention to process pupils' biometric data and emphasise that parents may object at any time to the processing of the information.

TCAT will ensure that pupils' biometric data is not taken or used as part of a biometric recognition system if pupils under the age of 18 object or refuse to participate in activities that involve the processing of their biometric data. TCAT is aware that a pupil's objection or refusal overrides any parental consent to the processing of data.

TCAT will ensure that information is included in its privacy notices that explains how biometric data is to be processed and stored, including the rights available to individuals in respect of the processing.

Reasonable alternative arrangements will be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent or due to the pupil's own refusal to participate in the collection of their biometric data.

The alternative arrangements will ensure that pupils do not suffer any disadvantage or difficulty in accessing services and premises. Likewise, such arrangements will not place any additional burden on parents whose children are not participating in such a system.

9. Access

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed.

All disks and hard drives containing images belong to, and remain the property of, TCAT.

Individuals have the right to submit a SAR to gain access to their personal data in order to verify the lawfulness of the processing. SARs will be handled in accordance with TCAT's Subject Access Request (SAR) Policy.

Individuals have the right to have personal data erased if:

- The data is no longer necessary for the original purpose it was collected for
- They are relying on legitimate interests as a basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue the processing
- The data has been processed unlawfully
- There is a specific legal obligation

There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:

- Where the processing is needed for the performance of a task in the public interest or an official authority
- Certain research activities
- Compliance with a specific legal obligation

As an alternative to the right of erasure, individuals can limit the way their data is used if they have issues with the content of the data held by TCAT or they object to way it was processed.

Data can be restricted by either:

- Moving the data to another processing system
- Making the data unavailable to users
- Temporarily removing published data from a website

TCAT will verify the identity of the person making the request before any information is supplied.

TCAT will ensure that all recorded CCTV footage is stored securely to maintain its confidentiality, integrity and availability.

Access to CCTV footage will be strictly controlled. Only authorised members of staff will be permitted to view, retrieve or manage CCTV recordings. This will ensure that the rights of any recorded persons are protected at all times.

TCAT will regularly review access permissions to ensure they remain appropriate, particularly where staff roles change or individuals leave the organisation.

TCAT will implement appropriate technical and organisational measures to prevent unauthorised access to CCTV data. Where possible, footage will be encrypted. Where encryption is not in place, TCAT will ensure that alternative safeguards are applied, including:

- Restricting access to designated staff only
- Implementing appropriate security controls and safeguards
- Ensuring CCTV equipment and control rooms are physically secure
- Applying regular software updates and security patches

TCAT will ensure that all staff with access to CCTV systems:

- Are appropriately trained in the use of the system
- Understand their responsibilities in relation to data protection
- Are familiar with relevant school policies on the handling of personal data

Releasing the recorded images to third parties will be permitted only in the following limited and prescribed circumstances, and to the extent required or permitted by law:

- The police – where the images recorded would assist in a specific criminal inquiry
- Prosecution agencies – such as the Crown Prosecution Service (CPS)
- Relevant legal representatives – such as lawyers and barristers
- Persons who have been recorded and whose images have been retained where disclosure is required by virtue of data protection legislation and the Freedom of Information Act 2000

Requests for access or disclosure will be recorded, and the Chief Finance Officer will make the final decision as to whether recorded images may be released to persons other than the police.

10. Use of automatic number-plate recognition (ANPR)

TCAT does not currently use ANPR cameras on any TCAT site. This section is included should a new entrant to TCAT have such facilities in place.

If circumstances require it, TCAT may consider the use of Automatic Number Plate Recognition (ANPR) systems within our car parks. As these systems collect and process personal data in real time, their use will be carefully assessed to ensure it is necessary and proportionate.

Where used, ANPR systems will capture vehicle registration numbers, along with the date, time and location of entry or exit. This information will be treated as personal data, as it can be linked to identifiable individuals.

Prior to implementing any ANPR system, TCAT will complete a DPIA to assess risks and ensure compliance with data protection legislation. TCAT will ensure that only data necessary for the stated purpose is collected.

Where in use, clear and prominent signage will be displayed to inform individuals that ANPR is in use and to provide details on how to contact TCAT with any queries regarding the processing of their data.

Monitoring and review

Lifespan of Policy: 3 Years

At any point this policy is updated or fully reviewed, it will be updated on the main TCAT website and will automatically update on all TCAT school websites simultaneously.

Where an annual check or other check results in minor changes, the Version History will be reviewed and updated with a change in the number following the decimal point, for example, v1.1 ⇒ v1.2. Where the policy is reviewed in full, then the number before the decimal point will change and reset, for example v1.4 ⇒ v2.0.

Any changes made by the CEO in collaboration with the Board Appointed Trustee will be passed to the Trust Board for ratification and subsequently be notified to Clerks to Local Governing Bodies and Headteachers/Heads of School.

The next scheduled full review date for this policy is 29th September 2029.

Date approved by the Board Appointed Trustee: 30th September 2026.

To be ratified and recorded in the minutes at the first Trust Board Meeting after 30th September 2026.

Trust Glossary

AA	Admissions Authority	H&S	Health and Safety
AAI	Adrenaline Auto-Injector (Epi Pen)	HoS	Head of School
ACM	Asbestos Containing Materials	HSE	Health and Safety Executive
AHT	Assistant Headteacher	ICO	Information Commissioners Office
AIR	Attendance Intervention Reviews	IDSR	Inspection Data Summary Report
APDR	Assess Plan Do Review Cycle	IHP	Individual Healthcare Plan
APIs	Application Programming Interfaces	IRMS	Information and Records Management Society
ASC	Autistic Spectrum Condition	IWF	Internet Watch Foundation
ASP	Analyse School Performance	KCSIE	Keeping Children Safe in Education
ATH	Academy Trust Handbook	KS1/2/3/4	Key Stage 1/2/3/4
BAME	Black, Asian and Minority Ethnic Backgrounds	LAC	Looked After Child
BAT	Board Appointed Trustee	LADO	Local Authority Designated Officer
BCP	Business Continuity Plan	LGB	Local Governing Body
BFR	Budget Forecast Return	LLC	Low-Level Concerns
CEO	Chief Executive Officer	LSA	Learning Support Assistants

CFO	Chief Financial Officer	MASH	Multi-Agency Safeguarding Hub
CIF	Condition Improvement Fund	MAT	Multi-Academy Trust
CIN	Child in Need	MFA	Multi-Factor Authentication
CLA	Children Looked After	MFL	Modern Foreign Language
CMIE	Child Missing in Education	NCSC	National Cyber Security Centre
COO	Chief Operating Officer	NoV	Note of Visit
COSHH	Control of Substances Hazardous to Health	NPQ	National Professional Qualifications
CP	Child Protection	PA	Persistent Absence
CPD	Continuing Professional Development	PAN	Published Admission Number
CPOMS	Child Protection Online Management System	PECR	Privacy and Electronic Communications Regulations
CSCS	Children's Social Care Services	PEP	Personal Education Plan
CSE	Child Sexual Exploitation	PEEP	Personal Emergency Evacuation Plan
CTIRU	Counter-Terrorism Internet Referral Unit	PEx	Permanent Exclusion
CWD	Children with Disabilities	PP	Pupil Premium
CYPMHS	Children and Young People's Mental Health Services	PPG	Pupil Premium Grant
DBS	Disclosure and Barring Service	PSHE	Personal, Social and Health Education
DDSL	Deputy Designated Safeguarding Lead	PSED	Public Sector Equality Duty
DfE	Department for Education	PTFA	Parent, Teacher and Friends Association

DHT	Deputy Headteacher	QA	Quality Assurance
DSE	Display Screen Equipment	RIDDOR	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations
DSL	Designated Safeguarding Lead	RHE	Relationships and Health Education
DPO	Data Protection Officer	RPA	Risk Protection Arrangement
EAL	English as an Additional Language	RSHE	Relationships, Sex and Health Education
ECT	Early Career Teacher	SA	Severely Absent
EDIB	Equality, Diversity, Inclusion and Belonging	SALT	Speech and Language Therapist
EHA	Early Help Assessment	SARC	Sexual Assault Referral Centre
EHENA	Education, Health and Care Needs Assessment	SBM	School Business Manager
EHCP	Education, Health and Care Plan	SCC	Standard Contractual Clause
EHE	Elective Home Education	SCITT	School-Centred Initial Teacher Training
ELSA	Emotional Literacy Support Assistant	SCR	Single Central Record
ESFA	Education and Skills Funding Agency	SDP	School Development Plan
EVC	Educational Visit Coordinator	SDQ	Strengths and Difficulties Questionnaire
EWOSSE	Education Welfare and Safeguarding Support Officer	SEF	Self-Evaluation Form
EYFS	Early Years Foundation Stage	SEMH	Social, Emotional, and Mental Health
FBV	Fundamental British Values	SENCO	Special Educational Needs Coordinator

FFT	Fischer Family Trust	SEND	Special Educational Needs and Disabilities
FGM	Female Genital Mutilation	SIP	School Improvement Partner
FGMPO	FGM Protection Order	SLA	Service Level Agreement
FOI	Freedom of Information	SLCN	Speech, Language and Communication Needs
FSM	Free School Meals	SLT	Senior Leadership Team
FTS	Find a Tender Service	SPOC	Single Point of Contact
GAG	General Annual Grant	STEM	Science, Technology, Engineering and Maths
GDPR	General Data Protection Regulation	TA	Teaching Assistant
GIAS	Get Information about Schools	TAC	Team Around the Child
HASH	Herefordshire Association of Secondary Heads	TCAT	Three Counties Academy Trust
HBA	Honour Based Abuse	TUPE	Transfer of Undertakings (Protection of Employment)
HR	Human Resources	VSH	Virtual School Headteacher