Staffordshire University Academies Trust

CCTV Policy

Last Reviewed	**June 2026**
Reviewed by	**Operations Director**
Approved by	**CEO and DPO**
Date of approval	**August 2026**
Policy owner	**Estates & Compliance Manager**
Location	**MS Teams**

This policy forms part of the Trust's wider governance, safeguarding, information governance and cyber security framework. Compliance with this policy will be monitored through Trust assurance, risk management and compliance arrangements, with significant concerns escalated through the appropriate governance channels.

Purpose

Staffordshire University Academies Trust recognises its responsibility to protect the safety, security and welfare of pupils, staff, visitors and others using its premises.

The Trust and its academies may use closed-circuit television and other video-surveillance systems where their use is lawful, necessary and proportionate. CCTV is used as a supporting security and safeguarding measure and will not be treated as a substitute for effective supervision, site security, risk management or safeguarding arrangements.

The purpose of this policy is to establish the arrangements for the installation, management, operation, monitoring and use of CCTV systems across Staffordshire University Academies Trust.

This policy is intended to ensure that:

- CCTV is used only for clear, specified and legitimate purposes;
- the need for CCTV is assessed before it is installed or materially changed;
- CCTV use is necessary and proportionate to the identified risk or need;
- individuals are informed when CCTV is operating;
- recorded images are relevant, adequate and suitable for the purpose for which they are collected;
- access to footage is appropriately restricted and controlled;
- footage is retained only for as long as it is required;
- requests for access to or disclosure of footage are handled lawfully; and
- CCTV systems and recorded information are protected by appropriate physical, technical and organisational security measures.

This policy applies to all academies and other premises operated by Staffordshire University Academies Trust that use CCTV or other video-surveillance systems.

Legislative and regulatory framework

This policy has been prepared having regard to the following legislation:

- UK General Data Protection Regulation;
- Data Protection Act 2018;
- Data (Use and Access) Act 2025;
- Protection of Freedoms Act 2012;
- Human Rights Act 1998;
- Freedom of Information Act 2000;
- Equality Act 2010;
- Regulation of Investigatory Powers Act 2000, where applicable;
- Children Act 1989;
- Children Act 2004; and
- Children's Wellbeing and Schools Act 2026, where applicable.

This policy also has regard to:

- Keeping Children Safe in Education 2026 (effective from 1 September 2026)

- Department for Education guidance, *Data protection in schools*, including guidance on taking and using photos and videos and using CCTV in schools;
- Department for Education guidance concerning the protection of children's biometric information;
- Information Commissioner's Office guidance on video surveillance, including CCTV;
- Information Commissioner's Office guidance on the UK GDPR and data protection in schools; and
- the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012, insofar as its principles are applicable or provide relevant good practice.

This policy should be read alongside the Trust's:

- Data Protection Policy;
- Information Security or Cyber Security Policy;
- Online Safety Policy;
- Freedom of Information Policy;
- Records Retention and Management Policy;
- Personal Data Breach Management Procedure;
- Safeguarding and Child Protection Policy;
- Staff Code of Conduct; and
- relevant Estates and Premises Management procedures

This policy operates in conjunction with the following school policies:

- Use of Images Policy
- Online Safety Policy
- Freedom of Information Policy
- GDPR Data Protection Policy

1 Objectives of the CCTV Policy

- To increase personal safety of staff, pupils/students and visitors and reduce the fear of crime;
- To protect SUAT buildings and their assets;
- To support the police in a bid to deter and detect crime;
- To assist in identifying, apprehending and prosecuting offenders;
- To assist in managing the academies and the investigation of suspected breaches of Academy/Trust regulation;
- To help ensure that those capturing individuals' information comply with the DPA 2018, UK GDPR and other such relevant statutory obligations;
- To contribute to the efficient deployment and operation of a camera system;
- To ensure that the information captured is usable and can meet its objectives in practice;
- To reduce reputational risks by staying within the law and avoiding regulatory action and penalties;
- To re-assure those whose information is being captured, of Academy compliance;
- To manage the risks of using CCTV systems to capture personal information.

This policy covers the use of surveillance and CCTV systems which capture moving and still images of people who could be identified, as well as information relating to individuals for any of the following purposes:

- Observing what an individual is doing.
- Taking action to prevent or detect a crime, damage to properties, violence or aggression towards premises occupants.

- Using images of individuals that could affect their privacy.

The surveillance system will be used to:

- Maintain a safe environment.
- Ensure the welfare of pupils, staff and visitors.
- Deter criminal acts against persons and property.
- Assist the police in identifying persons who have committed an offence.

2 Statement of intent

Surveillance camera systems are deployed extensively within the UK and where they are used appropriately, these systems are valuable tools which contribute to public safety and security and in protecting both people and property. The Trust and its academies seek to operate CCTV systems in a manner that is consistent with respect for the individual's privacy.

The majority of surveillance systems are used to monitor and/or record the activities of individuals and as such they process individuals' personal data. Academy use of surveillance systems involves the processing of personal data and will therefore be governed by the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 where applicable, and relevant current guidance issued by the Information Commissioner's Office.

The accountability principle requires academies using CCTV systems to take responsibility for the processing activities undertaken using personal data and to demonstrate compliance with the UK GDPR data protection principles. Appropriate measures and records must be maintained throughout the life of the processing.

Using surveillance systems can be privacy intrusive. They are capable of placing large numbers of law abiding people under surveillance and recording their movements as they go about their day to day activities. As such, academies will carefully consider whether or not to use a surveillance system and will take into account the nature of the problem they are seeking to address, inclusive of:

- Whether a surveillance system would be a justified and effective solution
- Whether better solutions exist
- What effect its use may have on individuals, and whether in the light of this, its use is a proportionate response to the problem

As such, SUAT and the academies will treat the systems and all information, documents and recordings obtained and processed as data which are governed by the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR). Cameras will be used to monitor activities within Academy premises; buildings, car parks and other such public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of ensuring the safety and wellbeing of Academy staff, pupils/students and visitors, alongside the security of the premises. It is likely that the majority of use of CCTV systems will be under the GDPR's lawful basis for processing – Public Task - Article 6(1)(e).

All planning and design has and will endeavour to ensure that the CCTV systems being used, 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.

The use of CCTV systems in academies will be regularly reviewed for effectiveness in accordance with their original purpose for siting. Cameras in situ will be subject to review at least on an annual basis.

CCTV which is not utilised for its original purpose in accordance with section one of this policy, or which is no longer effective, may be subject to decommission following reviews of usage.

It should be noted that CCTV is not utilised in all SUAT Academy buildings and external premises and therefore this policy only applies to those academies who operate CCTV systems.

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 the 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.

The Trust does not condone the use of covert surveillance when monitoring staff, pupils and others occupying the premises. 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

3.1 Staffordshire University Academies Trust

Staffordshire University Academies Trust is the Data Controller for personal data processed through CCTV systems operated by the Trust and its academies.
The Trust retains overall responsibility for ensuring that CCTV systems are operated in accordance with data protection legislation, this policy and other applicable legal requirements.

The Trust will:

- establish the governance framework for the use of CCTV;
- ensure that appropriate policies, privacy information and procedures are maintained;
- determine appropriate delegated authority for the approval and operation of CCTV systems;
- provide access to appropriate data protection advice;
- ensure that significant risks, breaches or concerns are escalated appropriately; and
- periodically monitor compliance with this policy.

3.2 The Data Protection Officer

The Data Protection Officer will provide independent advice and oversight in relation to the Trust's use of CCTV.

The Data Protection Officer will:

- advise on the lawful basis for processing CCTV information;
- advise on the necessity and proportionality of proposed CCTV use;
- advise on and monitor Data Protection Impact Assessments;
- provide advice on privacy notices, signage, retention and security;
- advise on subject access requests, requests for erasure, objections, restrictions and other data-subject rights;
- advise on requests for disclosure to the police, legal representatives or other third parties where required;
- advise on suspected personal-data breaches;
- make recommendations to the Trust and its academies regarding compliance; and
- support consultation with the Information Commissioner's Office where this is legally required.

3.3 The Chief Executive Officer

The Chief Executive Officer has executive oversight of this policy and will ensure that appropriate arrangements are in place across the Trust.

The Chief Executive Officer will only be required to approve an individual CCTV decision where:

- the matter presents a significant legal, safeguarding, financial or reputational risk to the Trust;
- covert surveillance is being considered;
- the proposed use involves facial recognition, biometric processing, automated decision-making or another particularly intrusive technology;
- disclosure to the media is being considered; or
- the matter has otherwise been escalated by the Data Protection Officer, Operations Director or Headteacher.

3.4 The Operations Director

The Operations Director is the policy owner and is responsible for overseeing the Trust-wide implementation of this policy.

The Operations Director will:

- ensure that appropriate central procedures and assurance arrangements are maintained;
- oversee the relationship between CCTV management, estates management, information security and data protection;
- ensure that significant CCTV installations or changes are appropriately authorised;
- support academies in resolving operational or compliance concerns; and
- report significant matters to the Chief Executive Officer or Trust Board as appropriate.

3.5 Headteachers

The Headteacher is responsible for the local implementation and day-to-day governance of CCTV within the academy.

The Headteacher will:

- ensure that CCTV is used only for approved purposes;
- ensure that the academy maintains accurate records of its CCTV arrangements;
- identify authorised system users and periodically review their access;

- ensure that staff with CCTV responsibilities receive appropriate instruction and training;
- ensure that privacy notices and signs are accurate, clear and visible;
- ensure that footage is retained and deleted in accordance with this policy;
- ensure that requests to view, preserve or disclose footage are properly recorded;
- ensure that faults, security incidents and suspected breaches are reported promptly;
- participate in the annual review of CCTV use; and
- consult the Data Protection Officer or Trust central team where required by this policy.

3.6 Designated Safeguarding Lead

The Designated Safeguarding Lead will be consulted where CCTV footage is relevant to a safeguarding concern or the welfare of a child.

The Designated Safeguarding Lead will:

- ensure that relevant CCTV footage is considered appropriately as part of safeguarding action or decision-making;
- ensure that relevant footage is preserved where there is a risk that it may otherwise be automatically deleted;
- advise, in conjunction with the Data Protection Officer where appropriate, on the lawful sharing of footage with children's social care, the police or other safeguarding agencies; and
- ensure that any safeguarding use or disclosure of CCTV footage is appropriately recorded.
- review whether CCTV arrangements remain effective in supporting safeguarding, child protection and pupil welfare, and where necessary recommend changes to camera locations, image quality, retention arrangements or operating procedures to address identified safeguarding risks;

The Designated Safeguarding Lead does not require unrestricted routine access to CCTV solely by virtue of their role. Access must be limited to what is necessary and proportionate for the particular safeguarding purpose.

3.7 School Office Managers and nominated CCTV coordinators

A Headteacher may delegate defined operational responsibilities to the School Business Manager or another suitably trained member of staff.

Delegated duties may include:

- maintaining the academy’s CCTV asset register;
- maintaining the authorised-user list;
- arranging routine maintenance and system checks;
- maintaining access, disclosure and deletion records;
- coordinating responses to requests for footage;
- checking that signs remain accurate and visible; and
- supporting the annual review.

Delegation of these duties does not transfer the Trust’s legal responsibility as Data Controller or the Headteacher’s responsibility for local implementation.

3.8 Authorised CCTV users

Only staff who have been expressly authorised by the Headteacher may access or operate the CCTV system.

Authorised users must:

- use the system only for an approved purpose;
- comply with this policy, the Staff Code of Conduct and data protection requirements;
- maintain strict confidentiality;
- prevent unauthorised persons from viewing footage;
- record access, downloads, copying and disclosure where required;
- immediately report any misuse, unauthorised access, loss or disclosure; and
- complete any required training.

3.9 IT support providers and contractors

IT support providers, security contractors and CCTV maintenance providers may access CCTV equipment or information only where this is necessary for an authorised purpose and appropriate contractual and security arrangements are in place.

Contractors must:

- be subject to appropriate confidentiality and data-processing obligations;
- access only the information required to perform their duties;
- comply with the Trust's security and site-access requirements;
- not retain, copy or disclose footage unless expressly authorised; and
- promptly report any suspected security incident or personal-data breach.

4 Purpose, justification and transparency

4.1 Approved purposes

CCTV may be used for one or more of the following specified purposes:

- protecting pupils, staff, visitors and other persons from harm;
- supporting safeguarding and welfare arrangements;
- preventing and detecting crime, antisocial behaviour, violence, aggression, vandalism and unauthorised access;
- protecting Trust buildings, equipment and other assets;
- supporting the management of emergencies, evacuations and lockdowns;
- investigating specific incidents, complaints or alleged breaches of Trust policies;
- assisting the police or another authorised body where disclosure is lawful and necessary; and
- securing evidence for legal, disciplinary, regulatory or insurance purposes where its use is lawful, necessary and proportionate.

CCTV must not be used for a purpose that is incompatible with the purpose for which the footage was originally collected unless the proposed further use is permitted by law.

4.2 Lawful basis

The Trust will identify and document an appropriate lawful basis before processing personal data through CCTV.

In most circumstances, the Trust will rely upon Article 6(1)(e) of the UK GDPR because the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.

Where public task is not applicable, the Trust may rely upon another lawful basis where this has been identified and documented following advice from the Data Protection Officer.
Consent will not ordinarily be relied upon because individuals cannot usually exercise a genuine choice about whether they are captured by CCTV.

Where CCTV processing is likely to capture special-category personal data, the Trust will identify an appropriate condition under Article 9 of the UK GDPR and Schedule 1 of the Data Protection Act 2018 where required.

4.3 Necessity and proportionality

Before installing CCTV or making a material change to an existing system, the academy must identify:

- the specific risk, problem or pressing need to be addressed;
- why CCTV is considered capable of addressing that need;
- whether a less intrusive measure could reasonably achieve the same outcome;
- the likely effect on the privacy and other rights of individuals;
- the proposed locations, fields of view and operating arrangements;
- who will have access to the system;
- how long footage will be retained; and
- the measures that will be used to reduce identified risks.

CCTV will not be installed or retained merely because the technology is available or as a general precaution where no identifiable need exists.

Children's wellbeing and best interests

In deciding whether CCTV is necessary, proportionate and justified, the Trust and its academies will have regard to the welfare, wellbeing, dignity, privacy and best interests of children.

The Trust is committed to ensuring that surveillance arrangements support an inclusive environment in which all pupils can feel safe, valued and able to participate fully in school life. Particular consideration will be given to the impact of CCTV on pupils with special educational needs and disabilities, medical needs or other vulnerabilities. Decisions regarding the installation, operation and review of CCTV systems will take account of equality, accessibility, inclusion, wellbeing and the individual needs of pupils.

Surveillance arrangements will seek to balance safeguarding, security and operational needs with children's rights and reasonable expectations of privacy. Particular consideration will be given where surveillance may affect vulnerable pupils, pupils with SEND or pupils receiving pastoral or safeguarding support.

4.4 Transparency

The Trust and its academies will be open and transparent about their use of CCTV.
Individuals will ordinarily be informed through:

- clearly visible signs positioned before they enter a monitored area;
- the relevant privacy notice;
- this policy; and
- additional communication where a new or materially changed system is likely to have a significant effect on pupils, staff, parents or visitors.

Signs must identify the Trust or academy operating the system, the principal purpose of the CCTV and a contact point through which further information may be obtained.

4.5 Locations in which CCTV will not ordinarily be used

CCTV will not ordinarily be installed in:

- toilets;
- changing rooms;
- shower or washing facilities;
- medical examination or treatment areas;
- rooms used for counselling or confidential meetings; or
- any other location in which individuals have a heightened and reasonable expectation of privacy.

CCTV will not ordinarily be installed in classrooms for routine monitoring. Any exceptional proposal to use CCTV within a teaching or learning area must be supported by a clearly documented safeguarding or security need, a Data Protection Impact Assessment and prior approval from the Data Protection Officer and Chief Executive Officer.

CCTV will not be used for routine monitoring of staff performance, attendance, productivity or teaching quality.

5 Operation of the System

5.1 The CCTV system will be administered under the authority of the Headteacher, who may nominate suitably trained staff to undertake defined operational duties. Access will be restricted to staff whose duties require it.

5.2 Each camera must have a specified and documented purpose. Cameras will be located and configured so that they capture only images that are adequate, relevant and necessary for that purpose. The system may operate continuously where this is justified by the identified purpose, although footage will not ordinarily be continuously watched through live monitoring.

5.3 In accordance with the Surveillance Camera Code of Practice, CCTV System operators should adopt the following guiding principles:

- *Use of a surveillance camera system must always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need.*
- *The user of a surveillance camera system must take into account its effect on individuals and their privacy, with regular reviews to ensure its use remains justified.*
- *There must be as much transparency in the use of a surveillance camera system as possible, including a published contact point for access to information and complaints, this will usually be via the Academy's privacy notices.*
- *There must be clear responsibility and accountability for all surveillance camera system activities including images and information collected, held and used.*

- *Clear rules, policies and procedures must be in place before a surveillance camera system is used, and these must be communicated to all who need to comply with them.*
- *No more images and information should be stored than that which is strictly required for the stated purpose of a surveillance camera system, and such images and information should be deleted once their purposes have been discharged.*
- *Access to retained images and information should be restricted and there must be clearly defined rules on who can gain access and for what purpose such access is granted; the disclosure of images and information should only take place when it is necessary for such a purpose or for law enforcement purposes.*
- *Surveillance camera system operators should consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards.*
- *Surveillance camera system images and information should be subject to appropriate security measures to safeguard against unauthorised access and use, both physically and technically.*
- *There should be effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with in practice, and regular reports should be published.*
- *When the use of a surveillance camera system is in pursuit of a legitimate aim, and there is a pressing need for its use, it should then be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value.*
- *Any information used to support a surveillance camera system which compares against a reference database for matching purposes should be accurate and kept up to date.*

5.4 CCTV footage may be viewed, retrieved, downloaded, copied or otherwise managed only by staff authorised by the Headteacher. The academy must maintain an up-to-date record of authorised users and their level of access. Access must be removed promptly when it is no longer required, including when an employee changes role or leaves the Trust.

5.5 The CCTV systems will be used to observe Academy premises and areas under surveillance in order to identify incidents requiring a response. Any response should be proportionate to the incident.

5.6 Cameras must be positioned, masked or configured, so far as reasonably practicable, to avoid capturing private homes, gardens and other areas outside the academy's responsibility. Where some incidental capture is unavoidable, the academy must document why this is necessary and what privacy-reducing measures have been applied.
Staff must not deliberately direct or use a camera to monitor a particular individual or group outside the approved purposes of the system. Any proposal involving targeted or covert monitoring must be referred immediately to the Data Protection Officer and must not commence without the required legal assessment and written authorisation.

5.7 CCTV will not be used for routine performance management or general monitoring of staff. Footage may, however, be considered in relation to a specific incident, safeguarding concern, complaint, alleged misconduct or other formal investigation where its use is lawful, relevant, necessary and proportionate. Any such use must be handled under the relevant Trust procedure and with appropriate advice from Human Resources or the Data Protection Officer.

5.8 CCTV footage will not be used for commercial or entertainment purposes and will not ordinarily be released to the media.
Any proposed disclosure to the media must relate to a legitimate and specific purpose, be lawful, necessary and proportionate, and be approved by the Chief Executive Officer following consultation with the Data Protection Officer and, where appropriate, the police or legal advisers.

5.9 Each academy operating CCTV must maintain:

- an up-to-date plan showing the location and field of view of each camera;

- a CCTV asset register;
- information asset ownership records, security classification details and nominated information asset responsibility arrangements for CCTV systems and associated recordings, in accordance with the Trust's information governance and cyber security framework;
- an authorised-user list;
- a record of the purpose and justification for each camera;
- the applicable retention period;
- maintenance and security-check records; and
- access and disclosure records.

These documents must be reviewed whenever a camera is installed, moved, removed, reconfigured or used for a materially different purpose.

5.10 Appropriate signage must be displayed before individuals enter areas covered by CCTV. Signage must comply with the transparency requirements set out in this policy and the Trust's applicable privacy information and must remain clear, accurate and visible.

5.11 The Trust does not routinely undertake covert surveillance.

Covert surveillance may be considered only in exceptional circumstances involving a specific and serious concern, where there are reasonable grounds to believe that overt measures would prejudice the investigation and where the proposed action is necessary and proportionate.

No covert surveillance may take place without:

- written approval from the Chief Executive Officer;
- advice from the Data Protection Officer;
- completion of an appropriate Data Protection Impact Assessment;
- consideration of employment, safeguarding and human-rights implications;
- legal advice where appropriate;
- clearly defined limits on its purpose, location, duration and authorised users; and
- arrangements for review, retention and deletion.

Where the DPIA identifies a high residual risk that cannot be mitigated, the Trust will consult the Information Commissioner’s Office before processing begins.

Where covert or targeted surveillance is proposed, the Trust will obtain appropriate legal advice before surveillance begins to establish the applicable statutory framework, including whether the Regulation of Investigatory Powers Act 2000 or any other surveillance legislation applies. Any authorisation, review or record required by law will be completed using the current statutory or Trust-approved documentation applicable at the time.

Academy staff must not independently commence covert or directed surveillance or seek to rely on the Regulation of Investigatory Powers Act 2000 without prior approval from the Chief Executive Officer and advice from the Data Protection Officer and, where appropriate, legal advisers.

5.12 Specific purposes for the processing of personal data and use of CCTV information must be defined and communicated to those operating the systems. Data must be processed lawfully, fairly, and in a manner that people would reasonably expect, taking into account advancements in technology that may not be anticipated by some people.

5.13 Each academy must maintain written local arrangements covering:

- the staff authorised to access the system;
- the access level granted to each authorised user;
- the locations from which footage may be viewed;
- arrangements for downloading, copying, preserving and deleting footage;
- the process for dealing with subject access and third-party requests;

- system maintenance and fault reporting;
- security measures;
- incident and breach reporting; and
- the academy's retention period.

CCTV information will not be accessed, used or shared without a documented and lawful purpose.

5.14 A Data Protection Impact Assessment must be completed before:

- installing a new CCTV or surveillance system;
- adding cameras to an existing system;
- materially changing a camera's location, field of view or purpose;
- introducing audio recording;
- introducing ANPR, facial recognition, biometric processing, behavioural analytics or other automated functions;
- introducing remote or cloud-based monitoring or storage where this materially changes the risk; or
- undertaking any other surveillance processing likely to result in a high risk to individuals.

The DPIA must:

- describe the nature, scope, context and purpose of the processing;
- identify the lawful basis;
- assess necessity and proportionality;
- identify risks to individuals;
- consider whether an Equality Impact Assessment is required and whether the proposed surveillance may have a disproportionate impact on individuals or groups with protected characteristics;
- record measures to eliminate or reduce those risks;
- identify consultation undertaken; and
- record approval and review arrangements.

The DPIA must be reviewed when the nature, scope, context, purpose or risk of the processing changes.

5.15 The information the surveillance system processes must be of good quality and be adequate, relevant and limited to what is necessary. Academies must identify the minimum amount of personal data they need to fulfil their purpose(s) for processing the data.

5.16 Both fixed and mobile cameras must be focussed on a relevant space, and where wider surveillance is possible but unnecessary, this should be restricted. This ensures that surveillance does not occur in areas which are not of interest and individuals are not unintentionally made the subject of surveillance.

5.17 The Trust will not routinely use facial recognition, biometric identification, behavioural analytics, emotion recognition, automated categorisation or other artificial-intelligence functions as part of its CCTV systems.

Any system containing such functionality must have the functionality disabled unless its proposed use has been separately assessed and expressly approved. Before any such technology is enabled, the Trust must:

- identify a clear lawful and operational need;
- consider less intrusive alternatives;
- complete a Data Protection Impact Assessment;

- identify any applicable Article 9 UK GDPR condition;
- consult the Data Protection Officer;
- obtain approval from the Chief Executive Officer; and
- provide appropriate privacy information and safeguards.

The use of automated technology must not result in a significant decision being made about an individual solely by automated means unless this is permitted by law and appropriate safeguards are in place.

The ICO's surveillance guidance expressly covers CCTV, ANPR, facial recognition and other surveillance technologies.

5.18 Purpose limitation and further processing
CCTV information will be collected for specified, explicit and legitimate purposes and will not be further processed in a manner that is incompatible with those purposes.

Before CCTV information is used for a new purpose, the Trust or academy will consider whether the proposed further processing is compatible with the purpose for which the information was originally collected and whether an appropriate lawful basis and safeguards apply.
Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes will be managed in accordance with applicable data-protection legislation and appropriate safeguards.

5.19 Those under surveillance should clearly be aware that they are being recorded. Academies should provide individuals with appropriate information about how they can exercise their rights, and that appropriate restrictions on viewing and disclosing images are in place for those using the system. In SUAT academies, this would usually be provided through signage and privacy notices. It is important that signs are placed prominently before the entrance to the system's field of vision and for this to be reinforced with further signs inside the area. Information should be positioned at a reasonable distance from the places monitored, and in such a way that individuals can easily recognise the circumstances of the surveillance before entering the monitored area.

Where processing is not obvious to an individual, a sign could read "Images are being monitored and recorded for the purposes of crime prevention and public safety. This system is controlled by XXXXX. For more information, visit our website at (web address) or call XXXXXX."

5.20 The reasons for selecting a particular surveillance system should not be based solely on technical capabilities, including the quality of the images it can produce, the field of vision it offers or the amount of data it can record. Academies must also consider the governance capabilities that complement the system, such as software that enables footage to be uploaded, stored and audited. Personal data should be easily retrievable in response to a subject access request and other individual rights. Academies should ensure that their systems have the capability to redact footage if third parties need to be blurred or obscured.

5.21 Data collected from CCTV should be 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.

5.22 Data should be 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.

5.23 Data should be 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.

5.24 Surveillance and CCTV systems will be designed, positioned and operated so as to minimise unnecessary intrusion into individuals' privacy and will only be used where necessary and proportionate to the identified purpose.

Individuals should, so far as reasonably practicable, be able to understand:
• when they are being monitored by a surveillance camera system;
• who is responsible for operating the system; and
• the purposes for which the associated information is being processed.

5.25 Academies using CCTV should ensure that their signage is compliant by:

- Ensuring that signage is clear and visible, e.g. outdoor signs are not covered by overhanging branches.
- Ensuring that signage is an appropriate size, e.g. if the CCTV is located near a drop off point it needs to be big enough for driver to see it from inside a car.
- Ensuring that, if it captures images outside the Academy site, signs are clearly displayed for pedestrians.
- Ensuring that staff know who to talk to if they get asked about the images captured on CCTV.[1]

Furthermore, when creating CCTV in operation signs, the wording used must include:
- The details of the organisation operating the system.
- The purpose of its use, e.g. crime prevention.
- Who to contact if individuals have any enquires pertaining to the images being captured by the CCTV.

6 Data protection

CCTV images that identify or are capable of identifying an individual constitute personal data and will be processed in accordance with the UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025.

The Trust and its academies will ensure that CCTV information is:
- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- sufficiently accurate and of an appropriate quality for its intended purpose;
- retained for no longer than is necessary;
- protected against unauthorised or unlawful processing and against accidental loss, destruction or damage; and
- managed in a manner that enables the Trust to demonstrate compliance.

A Data Protection Impact Assessment will be completed and approved where required by Section 5.14 of this policy.

Where a DPIA identifies a high risk that cannot be adequately reduced, the Trust will consult the Information Commissioner’s Office before the processing begins.

CCTV footage will ordinarily be retained for no longer than 30 calendar days. Footage may be retained beyond the ordinary period where it is required for:

- a safeguarding investigation;
- a complaint or disciplinary investigation;
- the prevention or detection of crime;
- legal proceedings;
- an insurance claim;
- a subject access request;
- a request from the police or another authorised body; or
- another documented and lawful purpose.

  Footage retained beyond the ordinary period must be isolated or protected from routine deletion, securely stored, access-restricted and deleted when the reason for its continued retention ends.

  The Trust will not use live facial-recognition technology or routinely record audio. Equipment containing these functions must have them disabled by default.

7 System Access, monitoring and security

7.1 Live monitoring

CCTV footage will not ordinarily be continuously monitored live.

Live monitoring may be used where it is necessary for a defined security, safeguarding or emergency purpose. Live monitoring must be undertaken only by authorised staff and must not be used for general or speculative observation of individuals.

7.2 Secure viewing

CCTV screens and recordings must be viewed only in a secure location where they cannot be seen or overheard by unauthorised persons.

Screens must be locked, switched off or otherwise made inaccessible when not in authorised use.

7.3 User access

Each user must have an individual account wherever the system permits. Shared accounts must be avoided unless there is no reasonable technical alternative and additional controls are documented.

Access must be based on the minimum level required for the user's duties. Permissions must be reviewed at least annually and whenever a user changes role or leaves the Trust.

7.4 Passwords and authentication

CCTV systems must be protected by strong, unique passwords or passphrases in accordance with the Trust's Information Security or Cyber Security Policy.

Default manufacturer usernames and passwords must be changed before the system is placed into service.

Multi-factor authentication must be enabled wherever it is technically supported and proportionate.

Passwords must not be shared or displayed. A password must be changed immediately where compromise is known or suspected.

7.5 Network and device security

Network-connected CCTV systems must be subject to appropriate technical security controls. These will include, where applicable:

- secure configuration;
- network segregation;
- firewall protection;
- removal or disabling of unnecessary services and accounts;
- supported and appropriately patched firmware and software;
- encrypted communications;
- secure remote-access arrangements;
- malware protection where applicable;
- audit logging; and
- monitoring for unauthorised access.

CCTV systems must not be accessible through personal devices unless expressly authorised and protected through Trust-approved security controls.

7.6 Physical security
Recording equipment, servers, network video recorders, digital video recorders and associated control equipment must be located in a secure area. Physical access must be restricted to authorised persons.
Contractors requiring physical access must be appropriately authorised, supervised where necessary and informed of their confidentiality and security obligations.

7.7 System updates and maintenance
CCTV equipment must be maintained in accordance with manufacturer recommendations and the Trust's information-security arrangements.
Security updates and firmware patches must be assessed and applied within an appropriate period, taking account of the severity of the vulnerability and the operational effect of the update.
Unsupported equipment must be risk-assessed and replaced or otherwise appropriately mitigated.

7.8 Image quality and time settings
Cameras must provide images of sufficient quality for their documented purpose. The academy must check that:

- the image remains clear;
- the camera remains correctly positioned;
- the field of view has not been obstructed or altered;
- privacy masking remains effective;
- date and time settings are accurate; and
- recording and deletion functions operate correctly.

7.9 Routine checks
Academies must undertake and record:

- routine operational checks at an interval appropriate to the system and risk;
- periodic checks of security, access and system functionality;
- checks following significant maintenance, configuration changes or security incidents; and
- a formal annual review under Section 10.

Faults that could compromise security, privacy or evidential quality must be reported promptly and addressed within an appropriate period.

7.10 Copying and downloading
The ability to download, export or copy CCTV footage must be restricted to specifically authorised users.
Any download, copying, preservation or disclosure must be recorded, including:

- the date and time;
- the identity of the person undertaking the action;
- the footage concerned;
- the purpose;
- the lawful authority or approval; and
- the recipient, where applicable.

7.11 Staff responsibilities
Staff authorised to access CCTV must receive appropriate training and understand that deliberate misuse, unauthorised access, copying or disclosure may result in disciplinary action and may also constitute a criminal offence.

8 Installation, relocation and material alteration of CCTV systems

8**.1** No CCTV system or additional camera may be installed, relocated, materially reconfigured or used for a new purpose unless a clear operational need has been identified and the proposal has been assessed for necessity and proportionality.

8.2 Before approval is given, the academy must complete or update:

- a Data Protection Impact Assessment;
- the CCTV asset register;
- the camera-location plan;
- the applicable privacy notice;
- signage arrangements;
- the lawful-basis assessment;
- security and access arrangements;
- retention arrangements; and
- any required estates, electrical, fire-safety, safeguarding or contractor documentation.

Where a new CCTV system or a significant expansion or material change to an existing system is proposed, the academy will undertake proportionate consultation with affected pupils, parents/carers and staff where appropriate. The nature and extent of consultation will reflect the scale, location, purpose and privacy impact of the proposed surveillance.

The outcome of any consultation will be considered as part of the Data Protection Impact Assessment and approval process.

8.3 Proposed installations and material changes must be submitted to the Operations Director or another nominated Trust officer for operational approval following consultation with the Data Protection Officer.

8.4 Chief Executive Officer approval is required where the proposal:

- presents a significant legal, safeguarding or reputational risk;
- involves monitoring in an area where individuals have a heightened expectation of privacy;
- involves audio, biometric processing, facial recognition, artificial intelligence or automated analytics;
- involves covert surveillance; or
- is otherwise escalated by the Data Protection Officer or Operations Director.

8.5 CCTV installation and alteration work must be managed through the Trust's estates and contractor-management arrangements. Appropriate consideration must be given to:

- electrical safety;
- fire safety;
- asbestos information;
- work at height;
- safeguarding and contractor access;
- network and cyber security;
- planning or landlord consent where applicable; and
- the Construction (Design and Management) Regulations 2015 where the work falls within their scope.

8.6 Following installation, the system must be tested before being placed into operational use. The asset register, camera plan, user permissions, privacy notice and signage must be confirmed as accurate.

9 Protocols

The Trust will maintain any registration and pay any data protection fee required by law to the Information Commissioner's Office. CCTV processing will be incorporated within the Trust's data-protection governance arrangements, including its records of processing activities and applicable Data Protection Impact Assessments.

Appropriate CCTV signage will be displayed prominently before individuals enter areas covered by surveillance. Signs will be clear, visible and appropriate to the circumstances and will identify the organisation operating the system, the purpose of the surveillance and a means of obtaining further information. Additional or more prominent signage will be used where surveillance would be less reasonably expected.

The surveillance system has been designed for maximum effectiveness and efficiency; however, the school 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 the school.

10 Review of System Usage

10.1 Each academy operating CCTV must undertake and record a formal review at least annually. The review must be documented using the Trust's current CCTV review arrangements or other approved compliance documentation.

10.2 The review must consider:

- whether the original need for the CCTV system remains;
- whether each camera remains necessary and proportionate;
- whether a less intrusive measure could now achieve the purpose;
- whether each camera remains correctly located and configured;
- whether the field of view captures any unnecessary area;
- whether signage and privacy information remain accurate;
- whether the lawful basis remains appropriate;
- whether the Data Protection Impact Assessment remains current;
- whether the retention period remains justified;
- whether access permissions remain appropriate;
- whether maintenance, firmware and security updates are current;
- whether any supplier, processor, cloud-storage or maintenance arrangements remain appropriate and whether applicable contracts and data-processing arrangements remain current;
- whether the operation of the system has resulted in, or creates a risk of, disproportionate impact on any particular group of individuals and whether any equality implications require further assessment;
- whether any faults, breaches, complaints or requests indicate a need for change;
- whether trends in safeguarding incidents suggest that CCTV arrangements continue to support the effective safeguarding, welfare and protection of pupils;
- whether complaints relating to surveillance, privacy, data protection or the use of CCTV identify any areas requiring improvement;
- whether subject access requests, police requests, safeguarding disclosures or regulatory enquiries indicate any weaknesses in procedures, controls or staff training;
- whether changes in legislation, statutory guidance, safeguarding requirements, cyber security expectations or surveillance technology require amendments to this policy, related procedures or CCTV system configurations.
- whether the system continues to provide images of sufficient quality;
- whether the academy's asset register and camera plan are accurate; and
- whether any cameras should be removed, relocated or decommissioned.

10.3 The review must be approved by the Headteacher and retained as part of the academy's compliance records. Significant concerns or proposed material changes must be referred to the Operations Director and Data Protection Officer.

10.4 A camera that no longer serves an identified, lawful and proportionate purpose must be switched off, removed or reconfigured within a reasonable period.

10.5 A review must also be undertaken before the scheduled annual review where:

- the purpose or operation of the system changes;
- a camera is added, moved or materially reconfigured;
- new surveillance technology or functionality is proposed;
- a significant complaint or personal-data breach occurs; or
- there is another material change in risk.

11 Security, storage and audio recording

11.1 General security

The Trust and its academies will implement appropriate physical, technical and organisational measures to protect CCTV systems and footage from:

- unauthorised access;
- unlawful use or disclosure;
- accidental loss or deletion;
- alteration or corruption;
- theft or physical damage; and
- cyberattack or other compromise.

Access will be restricted to authorised users and will be managed in accordance with Section 7 of this policy.

11.2 Local storage

Where footage is stored locally, the recording equipment and storage media must be located in a secure area and protected by appropriate access controls.
Storage systems must be supported, appropriately configured and maintained. The academy must ensure that automatic deletion settings reflect the approved retention period.

11.3 Cloud-based storage or services

Cloud-based CCTV storage or management services may be used only where they have been approved through the Trust's procurement, information-security and data-protection arrangements.
Before a cloud service is implemented, the Trust must ensure that:

- appropriate supplier due diligence has been completed;
- the respective controller and processor responsibilities are documented;
- a compliant data-processing agreement is in place;
- footage is appropriately encrypted in transit and at rest;
- access is protected by suitable authentication controls;
- audit logs are available where appropriate;
- the location of data storage and any international transfers have been assessed;
- deletion, return and retention arrangements are contractually documented;
- sub-processors are identified and appropriately controlled;
- incident-reporting requirements are defined; and
- the Trust can retrieve, redact, preserve and delete footage as required.

The use of cloud storage must be recorded in the relevant Data Protection Impact Assessment and record of processing activities.

11.4 Remote access

Remote access to CCTV systems will be permitted only where it is operationally necessary, expressly authorised and protected through Trust-approved secure-access arrangements.
Remote access must not be enabled through default or unsupported manufacturer services and must not be undertaken using personal accounts or unmanaged personal devices.

11.5 Audio recording

CCTV systems operated by the Trust will not routinely record audio.
Where equipment has an audio-recording function, the function must be disabled by default.
Audio recording may be considered only in exceptional circumstances where:

- a specific and substantial need has been identified;
- less intrusive measures have been considered and found insufficient;
- the recording is necessary and proportionate;
- a lawful basis and any additional legal conditions have been identified;
- a Data Protection Impact Assessment has been completed;
- affected individuals will receive appropriate privacy information;
- recording can be limited to the minimum location and period required; and
- prior written approval has been obtained from the Chief Executive Officer following advice from the Data Protection Officer.

Continuous or indiscriminate recording of private conversations is prohibited.

11.6 Authorised users

Each academy must maintain a current list of authorised users, recording:

- the user's name and role;
- the level of access granted;
- the reason access is required;
- the date access was approved;
- the approving officer; and
- the date access was reviewed or removed.

The location of CCTV viewing monitors will be determined and documented by each academy within its local CCTV arrangements. Monitors must be located in secure areas and positioned or configured so that footage cannot be viewed by unauthorised persons.

12 Individual rights and subject access requests

12.1 Right of access

Individuals have the right to request access to personal data relating to them, including CCTV footage in which they can be identified.

Requests will be handled in accordance with the Trust's Subject Access Request procedure and applicable data protection legislation.

Where a request is made by a parent or carer for CCTV footage relating to a child, the Trust will consider whether the requester is entitled to exercise the child's data-protection rights on their behalf, taking account of the child's age, competence, circumstances and the nature of the request. Parental responsibility does not automatically provide an unrestricted right to receive CCTV footage containing the personal data of the child or other individuals.

12.2 Information required

- To enable the Trust to locate relevant footage, the requester may be asked to provide:

- the date and approximate time of the recording;
- the location;
- a description of themselves;
- details of the incident or circumstances; and
- appropriate evidence of identity.
- The Trust will request only the information reasonably required to locate the footage and verify the requester's identity.

12.3 Preservation of footage

Where a valid request relates to footage that may otherwise be automatically deleted, the academy must take reasonable steps to preserve the relevant footage pending consideration of the request.

Preserved footage must remain securely stored and access-restricted.

12.4 Third-party information

CCTV footage may contain the personal data of other individuals. Before footage is disclosed, the Trust will consider whether:

- the other individuals have consented to disclosure;
- it is reasonable to disclose without their consent;
- their identities can be obscured or redacted; or
- an exemption or restriction applies.

Where necessary, footage will be blurred, cropped, muted or otherwise redacted to protect the rights of other individuals.

12.5 Method of access

Depending upon the circumstances, access may be provided by:

- supplying a secure copy of the relevant footage;
- arranging supervised viewing; or
- supplying still images or another appropriate extract.

The method chosen must provide meaningful access while protecting the rights of other people and maintaining the security of the information.

12.6 Time for response and fees

The Trust will respond without undue delay and ordinarily within one month of receiving a valid request and any information reasonably required to verify identity and locate the footage.

The response period may be extended where permitted by law because of the complexity or number of requests. The requester will be informed of any extension and the reasons for it.

Requests will ordinarily be dealt with free of charge. A reasonable fee may be charged, or a request may be refused, only where permitted by data protection legislation, including where the request is manifestly unfounded or excessive.

12.7 Other rights

- Depending on the circumstances, individuals may also have rights to:
- request erasure;
- request restriction of processing;
- object to processing;
- request rectification of inaccurate associated information; and
- complain to the Information Commissioner's Office.
- These rights are not absolute. Requests will be considered in accordance with the applicable legal conditions, exemptions and the Trust's Data Protection Policy.
- Requests relating to these rights must be referred promptly to the Data Protection Officer.

13 Disclosure to the police and other third parties

13.1 General principle

- CCTV footage will not be disclosed to a third party unless there is a lawful basis for the disclosure and the disclosure is necessary, relevant and proportionate.
- The academy must not provide informal access to footage or permit a third party to photograph or record footage from a screen.

13.2 Permitted recipients

Subject to the circumstances and applicable law, footage may be disclosed to:

- the police or another law-enforcement body;
- a court, tribunal or other body acting under a legal power;
- the Crown Prosecution Service or another prosecution authority;
- the Trust's legal advisers;
- insurers or loss adjusters;
- safeguarding authorities;
- regulatory bodies;
- investigating officers appointed under a Trust procedure;
- individuals exercising their data-protection rights; or
- another person or organisation where disclosure is required or permitted by law.

Safeguarding disclosures

Where CCTV footage contains information relevant to the safeguarding or welfare of a child, the academy will ensure that relevant information is considered and, where necessary, shared appropriately and without unnecessary delay with the Designated Safeguarding Lead, local authority children's social care, the police or another relevant safeguarding agency.

Data protection legislation does not prevent the lawful sharing of information for the purpose of safeguarding and promoting the welfare of children. Concerns about data protection must not prevent or unnecessarily delay appropriate information sharing where this is necessary to protect a child.

Any disclosure must be relevant, necessary and proportionate to the safeguarding purpose and must be appropriately recorded.

13.3 Police requests

A request from the police should ordinarily be made in writing and must identify:

- the requesting officer and force;
- the footage required;
- the relevant date, time and location;
- the purpose of the request;
- the legal basis or policing purpose relied upon; and
- any urgency or preservation requirement.

An urgent verbal request may be considered where delay would create a significant risk to a person, the investigation or the evidence. The request and decision must be documented as soon as reasonably practicable.

13.4 Approval

Routine lawful disclosures may be authorised by the Headteacher or a nominated senior leader, following consultation with the Data Protection Officer where necessary.

Chief Executive Officer approval is required only where:

- the proposed disclosure presents a significant legal or reputational risk;
- disclosure to the media is proposed;
- the request is unusually broad or contentious;
- there is uncertainty about the lawful authority to disclose; or
- the matter has otherwise been escalated.

13.5 Disclosure record

Every disclosure must be recorded. The record must include:

- the date of the request;
- the requester’s identity and organisation;
- the information requested;
- the purpose and lawful basis;
- the decision and decision-maker;
- the footage disclosed;
- any redaction undertaken;

- the date and method of disclosure; and
- any conditions imposed on the recipient.

13.6 Secure transfer

Footage must be disclosed using an appropriately secure method. Where footage is copied to portable media or electronically transferred:

- it must be encrypted or otherwise appropriately protected;
- the recipient's identity and contact information must be verified;
- any password or access credential must be communicated separately;
- the transfer must be recorded; and
- only the minimum footage required must be provided.

13.7 Evidential footage

Footage required as evidence must be preserved in a manner that protects its integrity and maintains an appropriate audit trail.

- The record must show:
- when the footage was retrieved;
- who retrieved it;
- the source system and camera;
- the relevant date and time;
- any copies created;
- each person to whom it was transferred;
- the purpose of transfer; and
- its final return, deletion or disposal.

14 Storage, Retention and Deletion

14.1 CCTV footage will ordinarily be retained for no longer than 30 calendar days, unless an academy has documented a different period that is necessary and proportionate for the particular system and purpose.

14.2 Retention settings must be documented in the academy's CCTV asset register and Data Protection Impact Assessment.

14.3 Footage may be preserved beyond the routine retention period where it is reasonably required for:

- a safeguarding matter;
- a complaint or investigation;
- disciplinary or capability proceedings;
- the prevention or detection of crime;
- legal proceedings;
- an insurance matter;
- a subject access request;

- a regulatory request; or
- another lawful and documented purpose.

Where CCTV footage may contain evidence relevant to a safeguarding concern, an allegation involving an adult working with children, child-on-child abuse, a criminal investigation or another serious incident, the relevant footage must be preserved promptly once the academy becomes aware of its potential relevance.

Where CCTV footage may be relevant to an allegation, low-level concern, safeguarding concern, child-on-child abuse incident, serious behaviour incident or concern involving a member of staff, volunteer, governor, contractor or pupil, the relevant footage must be preserved promptly. Such footage must be handled in accordance with safeguarding requirements, allegations management procedures, disciplinary procedures and applicable data protection legislation. Access must be restricted to those with a legitimate need to know and an appropriate audit trail maintained.

Where the footage relates to the safeguarding or welfare of a child, the Designated Safeguarding Lead must be informed. Preservation of footage does not mean that it must ultimately be disclosed or retained indefinitely; continued retention must remain necessary, lawful and appropriately documented.

14.4 Where footage is preserved, the academy must record:

- the footage concerned;
- the reason for preservation;
- the person authorising preservation;
- the date on which preservation began;
- the people permitted to access it;
- the anticipated review or deletion date; and
- its eventual deletion or disposal.

14.5 Footage must be stored securely and protected by appropriate access controls. Encryption must be used where it is available and appropriate. Where encryption is not technically available, equivalent risk-reducing controls must be documented and applied.

14.6 Portable media may be used only where necessary and must:

- be Trust-owned or expressly approved;
- be checked and approved by the Trust's IT support arrangements;
- be encrypted wherever technically possible;
- be stored securely;
- be recorded in the disclosure or evidence log; and
- be securely erased or destroyed when no longer required.

14.7 Personal devices must not be used to access, photograph, record, download, store or transfer CCTV footage.

14.8 At the end of the relevant retention period, footage must be securely and irreversibly deleted unless continued retention is supported by a current and documented lawful reason.

15 Misuse, security incidents and personal data breaches

15.1 Any actual or suspected unauthorised access, viewing, use, copying, alteration, loss, deletion or disclosure of CCTV information must be reported immediately to the Headteacher and through the Trust's personal-data breach reporting procedure.

15.2 The Data Protection Officer must be informed promptly so that the Trust can assess:

- the nature and extent of the incident;
- the categories and number of individuals affected;
- the likely consequences;
- the measures required to contain and remedy the incident;
- whether affected individuals must be informed; and
- whether notification to the Information Commissioner's Office is required.

15.3 In operating CCTV systems, the Trust and its academies will have regard to the applicable principles of the Surveillance Camera Code of Practice, including necessity, proportionality, transparency, accountability, data minimisation, appropriate access controls, security and regular review. These principles are reflected throughout the requirements of this policy.

15.4 Evidence relating to the incident must be preserved where required. Access logs, system records and relevant footage must not be altered or deleted while an investigation is ongoing.

15.5 Deliberate or negligent misuse of CCTV by a member of staff may be addressed under the Trust's disciplinary procedures and may also constitute a criminal offence.

15.6 Following an incident, the Trust will identify and implement appropriate corrective action, which may include:

- changing access permissions;
- resetting credentials;
- updating software or system configuration;
- revising procedures;
- providing additional training;
- updating the DPIA;
- notifying affected parties;
- taking disciplinary or contractual action; or
- replacing or decommissioning equipment.

16 Assurance and compliance monitoring

The Trust may undertake proportionate assurance, compliance checks or audits of academy CCTV arrangements to confirm compliance with this policy. This may include reviewing CCTV asset registers, Data Protection Impact Assessments, authorised-user records, retention arrangements, access and disclosure logs, annual reviews, security controls, signage and training records.

Significant concerns identified through assurance activity will be referred to the Operations Director and Data Protection Officer and, where appropriate, escalated to the Chief Executive Officer or Trust Board.

17 Complaints and Queries

17.1 Any complaint about the operation or use of CCTV should normally be raised with the Headteacher of the relevant academy in the first instance. Complaints concerning the processing of personal data, the exercise of data-protection rights or alleged misuse or disclosure of CCTV information must also be referred promptly to the Trust's Data Protection Officer or relevant Data Protection Representative in accordance with the Trust's Data Protection Policy and privacy information.

Individuals also have the right to raise concerns with the Information Commissioner's Office where applicable.

17.2 Complaints will be investigated in accordance with SUAT's Complaints Policy and Procedures, Data Protection Policy and Retention and Records Management Policy.

18 Communication

18.1 All staff involved in the operation of CCTV systems will be made aware of this policy and will only be authorised to use the CCTV system in a way that is consistent with the purposes and procedures contained therein. Staff will be trained in compliance procedures as well as the use of the system itself.

18.2 All staff with responsibility for accessing, recording, disclosing or otherwise processing CCTV images must ensure that they are compliant with SUAT's data protection policies.

19 Publication and Freedom of Information Requests

19.1 This policy and relevant privacy information will be made available through the Trust or academy website.

19.2 Requests for recorded information about CCTV systems may fall within the Freedom of Information Act 2000. Such requests may include information about:

- the number or general location of cameras;
- the purposes for which systems are used;
- expenditure on CCTV;
- policies, procedures and impact assessments; or
- system-management arrangements.

19.3 A request for footage showing the requester will ordinarily be treated as a subject access request under data protection legislation rather than as a Freedom of Information request.

19.4 CCTV footage showing other identifiable individuals will constitute their personal data. Disclosure under the Freedom of Information Act is disclosure to the public generally and will therefore require careful consideration of the personal-information exemption and the data-protection principles.

19.5 Information will be disclosed unless a relevant exemption applies. Depending on the circumstances, exemptions may apply where disclosure would:

- disclose personal data unlawfully;
- prejudice the prevention or detection of crime;
- compromise the security of Trust premises or systems;
- breach an obligation of confidence; or
- otherwise cause a harm recognised by the Freedom of Information Act 2000.

19.6 Academies must refer requests involving CCTV footage, detailed camera locations, security arrangements or personal data to the person responsible for Freedom of Information requests and consult the Data Protection Officer before disclosure.

19.7 Freedom of Information requests will ordinarily be answered within 20 working days in accordance with the Trust's Freedom of Information Policy.

Monitoring and review

This policy will be reviewed at least annually by the Operations Director in consultation with the Data Protection Officer.

The review will take account of:

- changes to legislation and regulatory guidance;
- developments in surveillance technology;
- findings from academy annual CCTV reviews;
- complaints, incidents and personal-data breaches;
- subject access and disclosure requests;
- information-security risks;
- audit findings; and
- operational experience across the Trust.

Material amendments will be submitted through the Trust's policy-approval arrangements. Headteachers are responsible for ensuring that relevant changes are communicated to authorised CCTV users and incorporated into local procedures, privacy notices, training and system arrangements.

The next scheduled review date is: **August 2027**

APPENDIX A – Further guidance and resources

The Trust and its academies should refer to the most current versions of relevant statutory and regulatory guidance when operating or reviewing CCTV systems, including:

- Department for Education – Data protection in schools;
- Information Commissioner's Office – guidance on video surveillance, including CCTV;
- Surveillance Camera Code of Practice;
- Keeping Children Safe in Education; and
- Working Together to Safeguard Children.

Current versions of external guidance should be accessed from the issuing body's website rather than relying upon historic copies reproduced within this policy.