

CCTV AND VIDEO SURVEILLANCE POLICY

Policy Owner: Proprietor / CEO

Responsible Person: IT and CEO

Applies to: All TAS staff, students, contractors and visitors

Effective Date: September 2025 Review Date: September 2027

1. Purpose

TAS is committed to providing a safe and secure environment for students, staff and visitors.

Due to the individual needs and vulnerabilities of the children and young people attending TAS, CCTV is used as an additional safeguarding, health and safety and security measure.

The purpose of this policy is to ensure that CCTV is operated appropriately, proportionately and transparently and in accordance with applicable data protection legislation and guidance.

TAS recognises that CCTV footage may constitute personal data and therefore takes appropriate steps to protect the privacy and rights of individuals who may be captured by the system.

2. Purpose of CCTV

TAS CCTV is used for the following purposes:

- safeguarding and protecting students and young people;
- maintaining the safety and security of students, staff and visitors;
- preventing and identifying unauthorised access to the premises;
- assisting with the investigation of incidents and accidents;
- assisting with safeguarding investigations;
- investigating allegations where CCTV footage may be relevant;
- providing evidence to appropriate authorities where this is necessary and lawful.

CCTV is an additional safeguarding and security measure and does not replace appropriate supervision, risk assessments, safeguarding procedures or staff management processes.

3. Areas Covered by CCTV

TAS CCTV may operate in areas including:

- entrances and exits;
- corridors;
- communal areas;
- outdoor areas;
- access points;
- areas requiring additional security or safeguarding measures; and
- classrooms.

CCTV will not be positioned in areas where individuals have a reasonable expectation of privacy, including toilets, changing areas or other designated private areas.

Cameras will be positioned to capture the relevant area for the stated purpose and wherever reasonably practicable, to minimise unnecessary intrusion into individuals' privacy.

4. Classroom CCTV

TAS operates CCTV within classrooms because of the safeguarding and safety needs of the children and young people attending the school.

Classroom CCTV may be used to:

- investigate safeguarding concerns;
- investigate incidents or accidents;
- investigate allegations;
- establish what occurred during an incident;
- support the protection of students and staff; and
- provide evidence where this is necessary and proportionate.

The purpose of classroom CCTV is not to routinely monitor individual members of staff or to assess staff performance.

Classroom cameras should be positioned to capture the classroom environment rather than being deliberately directed towards a particular individual.

Staff may inevitably appear within classroom CCTV footage as part of normal classroom activity. This does not constitute targeted monitoring of staff.

CCTV will not ordinarily be used as a substitute for normal lesson observation, supervision, performance management or disciplinary procedures.

Where CCTV footage is relevant to a legitimate safeguarding, disciplinary, health and safety or other formal investigation, it may be reviewed in accordance with this policy.

5. Staff Monitoring

TAS recognises that staff members may be captured by CCTV while carrying out their normal duties. TAS will not use CCTV routinely to monitor staff performance, productivity or conduct.

TAS will not deliberately position or use CCTV for the purpose of placing an individual member of staff under continuous personal surveillance.

Where there is a specific and legitimate reason to review CCTV footage involving a member of staff, the footage may be reviewed where this is necessary and proportionate and where there is an appropriate lawful basis.

Any proposed use of CCTV for targeted or continuous staff monitoring will be subject to appropriate consideration of necessity, proportionality and data protection requirements.

6. CCTV Positioning and Maintenance

TAS CCTV cameras will be positioned to achieve the legitimate safeguarding, safety or security purpose for which they have been installed.

TAS-owned cameras will only be repositioned where there is an identifiable operational, safeguarding, security, maintenance or safety reason.

7. Third-Party and Landlord CCTV

CCTV equipment may also operate on or around TAS premises, which is owned or controlled by a third party, including the landlord.

Third-party CCTV does not form part of the TAS CCTV system.

Responsibility for the operation, recording, storage, retention, positioning and data protection compliance of third-party CCTV rests with the relevant owner or controller.

TAS staff must not interfere with, disable, reposition or alter third-party CCTV equipment unless authorised to do so by the relevant owner or as part of their authorised duties.

Where concerns are raised regarding third-party CCTV operating on the premises, TAS will seek clarification from the relevant owner or controller where appropriate.

8. Data Protection and ICO Registration

TAS recognises that CCTV footage may constitute personal data where individuals can be identified.

TAS will comply with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 and applicable data protection requirements.

TAS is registered with the Information Commissioner's Office (ICO) as a data controller and maintains the required data protection fee registration.

TAS will maintain its ICO registration and ensure that the relevant fee is renewed as required.

TAS will ensure that CCTV is operated in accordance with the data protection principles, including that footage is:

- processed lawfully, fairly and transparently;
- collected for specified and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- retained only for as long as necessary; and
- kept secure.

9. Lawful Basis

TAS will identify and document an appropriate lawful basis for its CCTV processing.

For routine CCTV used for safeguarding, security, protection of property and the prevention or investigation of incidents, TAS will generally consider legitimate interests as the appropriate lawful basis, where the necessary requirements are satisfied.

Where CCTV is used for a specific statutory, safeguarding, legal or public-interest purpose, TAS will consider whether another lawful basis is appropriate.

The applicable lawful basis will be documented within TAS's data protection records where required.

10. Transparency and Signage

TAS will ensure that individuals are appropriately informed that CCTV is operating on the premises.

Appropriate CCTV signage will be displayed in relevant areas.

CCTV signage will identify, where appropriate:

- that CCTV is operating;

11. Access to CCTV Footage

Access to CCTV footage will be restricted to authorised individuals who have a legitimate and appropriate reason to access it.

Authorised access may include the:

- Proprietor/Proprietress;
- CEO;
- Designated Safeguarding Lead;
- authorised members of the Senior Leadership Team; and
- designated CCTV/Data Protection personnel.

Access will be provided strictly on a need-to-know basis.

Not all members of the Senior Leadership Team will automatically have unrestricted access to CCTV footage.

CCTV footage must not be accessed simply out of curiosity or without a legitimate reason.

12. Downloading or Exporting CCTV Footage

CCTV footage will not routinely be downloaded, copied or exported internally.

Where there is a legitimate requirement for CCTV footage to be downloaded or exported, this must be:

1. necessary for an identified purpose;
2. authorised by the Proprietor/Proprietress or CEO before the footage is downloaded or exported; and
3. securely stored and managed in accordance with TAS's data protection requirements.

The person authorising the download/export and the reason for doing so should be recorded.

CCTV footage must not be copied to personal devices, personal email accounts, USB devices or other unauthorised storage locations.

13. Internal Use of CCTV Footage

CCTV footage may be reviewed internally where there is a legitimate reason, including:

- safeguarding concerns;
- incidents or accidents;
- allegations;

- health and safety investigations;
- complaints where CCTV is relevant;
- serious disciplinary matters where footage is directly relevant;
- suspected criminal activity; or
- other formal investigations authorised by TAS.

Any internal review must be limited to the footage reasonably required for the relevant purpose.

CCTV footage must not be used for purposes unrelated to the reason for which it was obtained.

14. Disclosure to External Agencies

CCTV footage will only be disclosed to external organisations where there is a lawful and legitimate reason to do so.

This may include formal investigations or requests from appropriate agencies such as:

- the Police;
- the Local Authority Designated Officer (LADO);
- safeguarding authorities;
- Ofsted or other relevant regulatory bodies;
- other statutory agencies; or
- legal or regulatory bodies where disclosure is required or otherwise lawful.

CCTV footage will not be shared simply because an individual, parent, staff member, professional or external organisation requests it.

Any request to disclose or provide CCTV footage externally must be referred to and approved by the Proprietor/Proprietress or CEO before disclosure, unless disclosure is required by law or an emergency safeguarding situation requires immediate action.

Where footage is disclosed, TAS will record:

- who received the footage;
- the date of disclosure;
- the reason for disclosure;
- the footage disclosed; and
- who authorised the disclosure.

Where appropriate, TAS may require the requesting agency to provide a formal request identifying the reason and legal basis for seeking the footage.

15. Subject Access Requests

Individuals have rights under data protection legislation in relation to their personal data.

An individual may make a Subject Access Request (SAR) where they believe their personal data is contained within CCTV footage.

All CCTV-related SARs must be referred to the person responsible for data protection at TAS.

TAS will consider the request in accordance with applicable data protection legislation, including the rights and privacy of other individuals who may appear within the footage.

CCTV footage will not be released automatically simply because an individual requests it.

16. Retention and Deletion

TAS CCTV footage will be retained for a maximum of 30 days.

At the end of the 30-day retention period, footage will be automatically overwritten or securely deleted in accordance with the CCTV system's technical configuration.

Where footage is required for a legitimate investigation, safeguarding matter, complaint, legal matter or formal request, relevant footage may be preserved beyond the normal 30-day retention period where this is necessary and lawful.

Any footage retained beyond 30 days must have a documented reason for continued retention and must be deleted once it is no longer required.

17. Security of CCTV Footage

CCTV footage must be stored securely and protected against:

- unauthorised access;
- unauthorised disclosure;
- accidental loss;
- unauthorised copying;
- alteration;
- misuse; and
- destruction.

Access credentials for CCTV systems must be kept confidential.

Any exported CCTV footage must be stored securely and must not be transferred or shared using unauthorised systems.

18. Data Protection Breaches

Any suspected:

- unauthorised access;
- unauthorised disclosure;
- inappropriate sharing;
- loss of CCTV footage;

- unauthorised downloading; or
- misuse of CCTV footage

must be reported immediately to the Proprietor/CEO or designated Data Protection Lead.

The incident will be managed in accordance with TAS's Data Breach Procedure.

Where necessary, TAS will assess whether the incident needs to be reported to the ICO or affected individuals.

19. Data Protection Impact Assessment

TAS will consider whether a Data Protection Impact Assessment (DPIA) is required where a new CCTV system is introduced or there is a significant change to the existing CCTV arrangements.

Particular consideration will be given where CCTV involves:

- systematic monitoring;
- monitoring of staff;
- monitoring of children and young people;
- audio recording;
- biometric technology; or
- other processing likely to result in a high risk to individuals.

The DPIA will consider necessity, proportionality, privacy, security, retention, access and any less intrusive alternatives.

20. Staff Responsibilities

All TAS staff must:

- comply with this policy;
- respect the privacy of students, staff and visitors;
- only access CCTV footage where authorised;
- maintain confidentiality;
- not copy or distribute CCTV footage without authorisation;
- not download footage without the required approval;
- report suspected misuse or data breaches immediately; and
- not interfere with CCTV equipment without authorisation.

21. Safeguarding

CCTV is an additional safeguarding tool and does not replace TAS's normal safeguarding procedures.

Where CCTV identifies or provides evidence of a safeguarding concern, the concern must be managed in accordance with the TAS Safeguarding and Child Protection Policy.

CCTV footage may form part of a safeguarding investigation where relevant.

Where a safeguarding concern requires external referral, CCTV footage may be shared with the appropriate statutory agency where there is a lawful basis for doing so and the disclosure has been appropriately authorised.

22. Children and Young People

TAS recognises that children and young people may be particularly vulnerable to inappropriate or excessive surveillance.

The school will therefore ensure that CCTV is used:

- for legitimate safeguarding, safety and security purposes;
- proportionately;
- transparently;
- securely; and
- only where necessary.

CCTV will not be installed in areas where children or young people have a reasonable expectation of privacy.

23. Complaints and Concerns

Any individual who has a concern regarding TAS's use of CCTV should raise the concern with the Proprietor/CEO or designated Data Protection Lead.

Concerns will be investigated appropriately.

Where the concern relates to personal data, the school's Data Protection Policy and complaints procedure will also apply.

TAS will cooperate with the Information Commissioner's Office where appropriate.

24. Monitoring and Review

TAS will periodically review its CCTV arrangements to ensure they remain appropriate and proportionate.

The review will consider:

- camera positioning;
- purpose and necessity;
- access arrangements;
- retention;
- security;
- signage;
- ICO registration;
- data protection requirements;

- DPIA requirements; and
- any relevant changes to legislation or ICO guidance.

This policy will be reviewed at least annually or sooner where there is a significant change to the CCTV system or relevant legal requirements.