

Shireland Collegiate Academy Trust Policy

CCTV Policy

Committee and Date Approved	Trust Board – Summer 2026
Category	Operational Regulations
Next Review Date	Annually – Summer 2027
Policy Availability	Trust Website

This policy reflects the guidance provided by the Shireland Collegiate Academy Trust for its Academies

Record of Amendments & Notable Changes to Legislation

[illegible]

1. Introduction

The Shireland Collegiate Academy Trust is fully committed to the safety of its staff, students, and visitors and to this extent has invested in the security of its buildings and facilities. The purpose of this policy is to regulate the management, operation, and use of the closed-circuit television (CCTV) system at our Academies

Common CCTV systems are based around digital technology and therefore need to be treated as information that will be processed under UK GDPR and Data Protection Act 2018. The person ultimately responsible for data protection within the Shireland Collegiate Academy Trust is the Chief Executive Officer (CEO).

The system comprises a number of fixed and dome cameras located both internally and externally around the Academy site. All cameras maybe monitored and are only available for use by approved members of staff. The Trust also uses a number of headcams/bodycams which are used to monitor specific serious incidents when deemed appropriate by approved staff.

The CCTV system is owned by the Trust and will be subject to annual review.

Objectives of the CCTV System

The objectives of the CCTV system are:

1. To protect the Trust buildings and its assets to ensure they are kept free from intrusion, vandalism, damage, or disruption.
2. To increase the personal safety of staff and students and reduce the fear of physical abuse, intimidation, and crime.
3. To support the police in a bid to deter and detect crime.
4. To assist in identifying, apprehending, and prosecuting offenders on the site.
5. To protect members of the public and private property.
6. To assist in the usage and management of the Academy building on a day-to-day basis.

Statement of Intent

1. The Trust will comply with the Data Protection Act 2018 and UK GDPR, whether it be information, recordings and downloads which relate to the CCTV system.
2. Cameras will be used to monitor activities within the Trust buildings, the car parks, and other areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of the

- occupants within each Academy, together with its visitors.
3. Staff have been instructed to ensure that static cameras will not focus on private homes, gardens, and other areas of private property.
 4. Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation from the Principal being obtained.
 5. Materials or knowledge secured as a result of CCTV system will not be used for any commercial purpose. Downloads will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Downloads will never be released to the media for purposes of entertainment.
 6. The planning and design of the existing CCTV system has endeavoured to ensure that the CCTV system will give maximum effectiveness and efficiency, but it is not possible to guarantee that the CCTV system will cover or detect every single incident taking place in the areas of coverage.
 7. Warning signs, as required by the Code of Practice of the Information Commissioner have been placed across our sites.

Operation of the System

The system will be administered and managed by the Principal, in accordance with the principles and objectives expressed in this policy.

1. The day-to-day management will be the responsibility of an appointed person at each site.
2. The CCTV system will be operated 24 hours each day, every day of the year.
3. The appointed person will check and log the efficiency of the system regularly to ensure the system is operational.
4. Access to the CCTV will be strictly limited to the members of staff approved by the Principal.
5. Unless an immediate response to events is required, staff must not direct cameras at an individual or a specific group of individuals.
6. The CCTV system may generate a certain amount of concern from members of the public. Any concern expressed by a member of the public should be referred to the Principal. If permission is granted by the Principal, the member of the public must be accompanied throughout the visit by a member of staff.
7. Any site visit by a member of the public may be immediately curtailed if the operational requirements of the CCTV System make this a necessity.
8. In the event of an emergency which requires an immediate contact with an emergency service to be contacted by a member of staff. The emergency procedures identified in the Health and Safety Policy will be adhered too.

Management of Access

1. Access to recorded CCTV images will be strictly controlled and limited to members of the Academy and Trust Leadership Teams, together with authorised individuals appointed by each Academy who have a legitimate and specific role in the management, investigation, or resolution of incidents.
2. Each CCTV system must be configured to ensure that only authorised users are able to access the system. Individual user accounts and unique login credentials must be assigned to each authorised person, and shared accounts or generic logins must not be used. CCTV systems must maintain an audit trail or activity log that records user access and actions undertaken, including where images are viewed, exported, or otherwise accessed. This enables the Academy to identify who has accessed CCTV footage and the purpose for which the access was required.
3. In some establishments, live CCTV monitoring is available within administrative offices to support the effective operation and safeguarding of the Academy, particularly within primary settings. Where live monitoring is in place, CCTV screens must be positioned so that they cannot be viewed by visitors, members of the public, or unauthorised individuals.
4. In circumstances where it is necessary, proportionate, and appropriate, CCTV images may be shown to pupils directly involved in an incident. This may be for the purpose of helping the pupil understand the impact of their actions, supporting restorative conversations, or as part of the Academy's behaviour management or disciplinary processes.
5. No other individual will be permitted to view, access, copy, or share CCTV images unless authorised in accordance with this policy and the relevant procedures governing the disclosure of CCTV footage.

Storage and Retention of Images

1. Any images recorded by the CCTV system will be retained only for as long as necessary for the purpose for which they were originally recorded.
2. Recorded images are stored for a maximum period of 31 days (where the system allows) unless there is a specific purpose for which they are retained for a longer period. In such circumstances authorisation for holding recorded images longer than 31 days must be sought from the Principal.
3. The Trust will ensure that appropriate security measures are in place to prevent the unlawful or inadvertent disclosure of any recorded images. The measures in place include:
 - a. CCTV recording systems being located in restricted access areas;
 - b. The CCTV system being encrypted/password protected with permissions

- based user access
 - c. Restriction of the ability to make copies to specified members of staff
4. A log of any access to the CCTV images, including time and dates of access, and a record of the individual accessing the images, will be maintained by the Trust.

Use of Personal Headcams/Bodycams

1. From time to time, personal cameras, known as headcams or bodycams, might be used to record major incidents within our Academy Campuses. These cameras are property of the Trust and are only used on our campuses. They are not routinely used and only switched on when staff are attending an incident which is deemed necessary to record.
2. Storage and use of any headcam footage will follow the same process as CCTV recordings.

Disclosure of Images to Data Subjects

1. Any individual recorded in any CCTV image is a data subject for the purposes of the Data Protection Legislation and has a right to request access to those images.
2. Any individual who requests access to images of themselves will be considered to have made a subject access request pursuant to the Data Protection Legislation. Such a request should be considered in the context of the Trust's Subject Access Request Policy.
3. When such a request is made a member of the Academy or Trust management or leadership team will review the CCTV footage, in respect of relevant time periods where appropriate, in accordance with the request.
4. If the footage contains only the individual making the request, then the individual may be permitted to view the footage. This must be strictly limited to that footage which contains only images of the individual making the request. The individual member of the Academy or Trust management or leadership team must take appropriate measures to ensure that the footage is restricted in this way.
5. If the footage contains images of other individuals, then the Trust must consider whether:
 - a. The request requires the disclosure of the images of individuals other

- than the requester, for example whether the images can be distorted so as not to identify other individuals;
 - b. The other individuals in the footage have consented to the disclosure of the images, or their consent could be obtained; or
 - c. If not, then whether it is otherwise reasonable in the circumstances to disclose those images to the individual making the request.
- 6. A record must be kept, and held securely, of all disclosures which sets out:
 - a. When the request was made;
 - b. The process followed by the Academy or Trust Management or Leadership team in determining whether the images contained third parties;
 - c. The considerations as to whether to allow access to those images;
 - d. The individuals that were permitted to view the images and when; and
 - e. Whether a copy of the images was provided, and if so to whom, when and in what format.

Disclosure of Images to Third Parties

If footage needs to be shared with a third party, a Data Sharing Request form must be completed. This request must receive approval from our Data Protection Officer (DPO) before any footage is disclosed. [S-CAT CCTV Third Party Viewing Form.docx](#)

1. The Trust will only disclose recorded CCTV images to third parties where it is permitted to do so in accordance with the Data Protection Legislation.
2. CCTV images will only be disclosed to law enforcement agencies in line with the purposes for which the CCTV system is in place.
3. If a request is received from a law enforcement agency for disclosure of CCTV images, then the member of the Academy or Trust Management or leadership must follow the same process as above in relation to subject access requests. Detail should be obtained from the law enforcement agency as to exactly what they want the CCTV images for, and any individuals of concern. This will then enable proper consideration to be given to what should be disclosed, and the potential disclosure of any third-party images.
4. The information above must be recorded in relation to any disclosure.
5. If an order is granted by a Court for disclosure of CCTV images, then this should be complied with. However, very careful consideration must be given to exactly what the Court order requires. If there are any concerns as to disclosure, then the Data Protection Officer should be contacted in the first

instance and appropriate legal advice may be required.

Review of Policy and CCTV System

1. This policy will be reviewed annually.
2. The CCTV system and the privacy impact assessment relating to it will be reviewed annually.
3. The entire CCTV system will be maintained by an approved contractor.

Misuse of CCTV systems

1. The misuse of CCTV system could constitute a criminal offence.
2. Any member of staff who breaches this policy may be subject to disciplinary action.

Complaints relating to this policy

Any complaints relating to this policy or to the CCTV system operated by the Trust should be made in accordance with the Trust Complaints Policy.

Summary of Key Points

- This CCTV Policy will be reviewed annually.
- The CCTV system is owned and operated by the Trust.
- The CCTV system cannot be accessed by visitors/ members of the public except by prior arrangement with the Principal and with good reason.
- Recordings may be viewed by data subjects / enforcement agencies and others provided the normal Subject Access Request procedure is followed.
- Copies will not be made available to the media for commercial or entertainment reasons.
- From time-to-time body worn cameras may be used to record serious incidents on site. These videos will be stored securely on our internal network and stored in line with this policy
- Any breaches of this policy will be investigated by the Principal. An independent investigation will be carried out for serious breaches.
- Breaches of the policy and recommendations will be reported to the Principal.
- The system will be maintained on a regular basis by an approved contractor.

Appendix 1 – Individual Academy Information/Checklist

Action	Information
Name of individual/s responsible for the operation of CCTV	<i>Conor Adderley (S-CAT)</i> <i>Mike Oakes (S-CAT)</i> Site Manager
Name of individual/s authorised to access CCTV	Principal Site Manager

Name of any external companies who also manage CCTV	
Has a DPIA been completed (this is only required for newly installed systems)/	
Do we have a map of camera locations available and who holds this?	
Are their appropriate signs around the Academy?	
Recording of all images by CCTV/Headcams are stored securely as per this policy. Access is limited to the following persons:	
How long are recordings stored for?	