Altrincham College

CCTV System Policy

Policy Date:	**October 2026**
Approved by Governors:	**October 2026**
Date of next review:	**October 2027**

Achieve + Learn Trust.

Better, together.

Contents

Background …….. page 3

Principles …….. page 3

Aims ……. page 3

Practice …… pages 4-5

- Operation of the CCTV system ……. page 4
- System functionality and access …….. page 4
- Location of Cameras …….. …….. page 4
- Liaison …….. page 5
- Video CD / DVD procedures / Storage device (e.g. USB) …….. page 4
- Breaches of the Code (including breaches of security) …….. page 5
- Access by the Data Subject …… page 5

Monitoring and Evaluation …… pages 5-6

- Monitoring procedures ……. page 5
- Assessment of scheme and code of practice …….. page 6
- Complaints ……. page 6
- Public information ……... page 6

Summary ……. page 6

Background

The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at Altrincham College, hereafter referred to as 'the school'.

The system comprises a number of fixed, dome and remote cameras located around the school site. All cameras are monitored via access to a secure system and are only available to selected staff with SLT approval and with SLT present.

The policy will be subject to review bi-annually to include consultation as appropriate with interested parties.

The CCTV system is owned by the school.

Principles

- To protect the school buildings and their assets.
- To increase personal safety and reduce the fear of crime.
- To support the Police in a bid to deter and detect crime.
- To assist in identifying, apprehending and prosecuting offenders.
- To protect members of the public and private property.
- To assist in managing the school.
- To be used in the legitimate interests of the school.

Aims

The CCTV system will seek to comply with the requirements of the Data Protection Act 2018, UK GDPR. In accordance with the Data Protection Act (2018) a data protection fee will be paid to the Information Commissioner.

The school will treat the system and all information, documents and recordings obtained and used as data which are protected by the Act and UK GDPR.

Cameras will be used to monitor activities within the school, its car parks and around the site to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the school, together with its visitors.

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 authorisation being obtained, as set out in the Regulation of Investigatory Power Act 2000.

Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. Recordings will only be released to the media for use in the investigation of a specific crime and with the written authority of the Police. Recordings will never be released to the media for purposes of entertainment.

The planning and design of the system have endeavoured to ensure that the Scheme 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.

Warning signs, have been placed at all access routes to areas covered by the school CCTV.

Practice

Operation of the CCTV system

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

The day-to-day management will be the responsibility of the Senior Leadership Team, ICT Network Manager and the Site Manager during the day and the Site Manager out of hours and at weekends.

The main CCTV system will be operated 24 hours each day, every day of the year.

Recordings are stored on hard drives for 30 days and are overwritten/wiped at this point, unless being retained for investigatory purposes.

System functionality and access

The ICT Network Manager will check and confirm the efficiency of the system daily and, in particular, that the equipment is properly recording and that cameras are functional.

Access to the CCTV system will be strictly limited to the SLT, ICT Network Manager and the Site Manager (Operators) within their designated area of work only.

Unless an immediate response to events is required, authorised staff (Operators) must not direct cameras at an individual or a specific group of individuals.

If concerns regarding safeguarding or health & safety are raised during viewing footage (regardless of the original reason the footage was accessed), these must be dealt with appropriately, following the usual systems and procedures.

Visitors and other contractors wishing to enter areas of work where images are being displayed will be subject to particular arrangements as outlined below.

Operators must satisfy themselves over the identity of any other visitors who view images and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be logged and signed off before recordings are viewed.

The system may generate a certain amount of interest. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Anyone wishing to use the system must first obtain permission from a member of SLT (or the Site Manager if at a weekend/out of hours) and be accompanied throughout the visit.

Any visit may be immediately curtailed if prevailing operational requirements make this necessary.

If out of hours emergency maintenance arises, the Operators must be satisfied of the identity and purpose of contractors before allowing entry.

Access to the servers (physically or remotely) is limited to the Operators via unique accounts which are password protected. Server rooms are secured both during the working day and when not staffed.

Other administrative functions will include maintaining recordings and hard disc space, filing and maintaining occurrence and system maintenance logs.

Emergency procedures will be used in appropriate cases to call the Emergency Services.

Location of Cameras

CCTV cameras will only be located in positions that are required for identified purposes. CCTV cameras will be positioned or masked to prevent monitoring and recording of any private property not belonging to the school.

CCTV cameras monitor the following locations 24 hours a day, 365 days a year:

- Points of entrance onto the school site
- Points of entrance into all school buildings
- Playgrounds and car parks
- Main school and Sixth Form reception areas
- Circulation areas (Corridors, stairwells etc.)
- Classrooms containing IT equipment

Liaison

Liaison meetings may be held with all bodies involved in the support of the system.

Media procedures / Storage device (e.g. USB Memory pen)

In order to maintain and preserve the integrity of the disks, optical or magnetic media used to record events from the hard drive and the facility to use them in any future proceedings, the following procedure for their use and retention must be strictly adhered to:

- Media required for evidential purposes must be sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store.
- If media is not copied for the Police before it is sealed, a copy may be made at a later date providing that it is then resealed, witnessed, signed by the controller, dated and returned to the evidence store.

Recordings may be viewed by the Police for the prevention and detection of crime or for supervisory purposes, authorised demonstration and training.

A record will be maintained of the release of media to the Police or other authorised applicants. A register will be available for this purpose.

Viewing of recordings by the Police must be recorded in writing and in the log book. Requests by the Police can only be actioned under the Data Protection Act or by Court Order.

Should a recording be required as evidence, a copy may be released to the Police under the procedures described above. Media will only be released to the Police on the clear understanding that the media remains the property of the school, and both the media and information contained on it are to be treated accordingly. The school also retains the right to refuse permission for the Police to pass to any other person the media or any part of the information contained thereon. On occasions when a Court requires the release of an original recording, this will be produced from the secure evidence store, complete in its sealed bag.

The Police may require the school to retain the stored media for possible use as evidence in the future. Such media will be properly indexed and properly and securely stored until it/they are needed by the Police.

Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Headteacher. In these circumstances, the media will normally be released

where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. In such a case, a reasonable fee will be charged for administrative costs, in relation to requests which are manifestly unfounded, manifestly excessive, or if further copies of data are requested.

Breaches of the code (including breaches of security)

Any breach of this policy by school staff will be initially investigated by the Headteacher or designated member of SLT, in order for them to take the appropriate disciplinary action.

Any serious breach will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

Access by the Data Subject

UK GDPR provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

Subject Access Requests should be made to the Headteacher. Individuals submitting requests for access will be required to provide sufficient information to enable footage relating to them to be identified, for example: photographic evidence, date, time and location.

Monitoring and Evaluation

The governing body is responsible for reviewing the CCTV System policy and procedures. The policy will be reviewed every year.

Monitoring Procedures

- Camera surveillance may be maintained at all times.
- Network Video Recorder hard drives are used to record images continuously.

Assessment of the scheme and code of practice

Performance monitoring, including random operating checks, may be carried out by the ICT Network Manager and the Site Manager.

Complaints

Any complaints about the school's CCTV system should be addressed to the Headteacher.

Complaints will be investigated in accordance with this Policy ('Breaches of the Code').

Public information

Copies of this Policy will be available to the public from the School Office and the Headteacher.

Summary:

- This Code of Practice will be reviewed every year.
- The CCTV system is owned and operated by the school.
- If concerns regarding safeguarding or health & safety are raised during viewing footage (regardless of the original reason the footage was viewed) these must be dealt with appropriately.
- Liaison meetings may be held with the Police and other bodies.
- Recording media will be used properly, indexed, stored and destroyed after appropriate use.
- Recordings may only be viewed by Authorised School Operators and the Police.
- Media required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.
- Recordings will not be made available to the media for commercial use or entertainment.
- Media no longer required will be disposed of securely.
- Any breaches of this code will be investigated by the Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Headteacher.