CCTV POLICY

Lead	**Director of IT**
Approved by Trust Board	**24 November 2022**
Full Review	**Autumn term 2025**

Introduction

The purpose of this policy is to regulate the management, operation and use of the Closed Circuit TeleVision (CCTV) at schools in The Collegiate Trust. This policy follows the guidelines published by the Home Office and the Information Commissioners Office (ICO) 2018 on the use of CCTV in public places.

CCTV Systems

CCTV is installed both internally and externally on school sites for the purpose of enhancing security of the buildings, property and associated equipment as well as creating a mindfulness among the occupants, at any one time that a surveillance security system is in operation within and in the external environs 24 hours a day.

- The CCTV system is owned and operated by The Collegiate Trust.
- The CCTV scheme is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The ICO registration number is ZA181155.
- The introduction of, or changes to, CCTV monitoring will be subject to consultation with senior leaders at each school.
- All authorised operators and employees with access to images are aware of the procedures that need to be followed when accessing the recorded images. All operators are reminded of the Data Protection Policy and applicable laws in their responsibilities under the CCTV Code of Practice. All employees are aware of the restrictions in relation to, and disclosure of, recorded images.
- CCTV warning signs must be clearly and prominently placed at all external entrances to each site, including access gates if coverage includes outdoor areas. CCTV notices must be placed on main building entrances.

CCTV surveillance at each school is intended for the purposes of:

- Protecting the school's buildings and assets at all times;
- Promoting a safe environment for staff, students and visitors;
- Preventing bullying;
- Reducing the incidence of crime and anti-social behaviour (including theft and vandalism);
- Supporting the Police and andy other official authorities where appropriate;
- Ensuring that the Trust and school rules are respected so that each school can be properly managed.

Summary of system capabilities:

- Fixed and Pan Tilt Zoom (PTZ) cameras of various models, sizes and colour are installed on the site;
- Any microphones embedded within cameras are disabled;
- The system does not have sound recording capability;
- Cameras are either configured to record continuously or when motion is detected;
- Some cameras have Infra-red capability to record in partial or total darkness;
- All footage is stored on central, managed and secure servers;
- Footage can accessed by authorised staff on designated workstations;
- Secure external access to the system by Premises Managers, Principals and IT System Administrators is permitted for the purpose of site safety and security;
- Access to specific cameras and recorded images is restricted according to the member of staff's role.
- The planning and design has endeavoured to ensure that the scheme gives maximum effectiveness and efficiency to cover general and vulnerable areas of the site. It is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.

Siting of cameras

- Cameras are sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy expectations are not violated.
- The Trust makes every effort to position the cameras so that their coverage is restricted to the school premises, which may include outdoor areas. In external areas, particularly around entrance gates, there may be some overspill to public rights of way. Every effort is made to avoid capturing images from other's private property.
- Any cameras positioned in a learning environment are sited for crime prevention, health & safety and safeguarding monitoring. They are not used to supervise staff.
- Members of staff should have access to details of where CCTV cameras are situated.
- The installation and maintenance of camera and CCTV systems may involve authorised 3rd party contractors. These works will be authorised and monitored by the Director of IT in partnership with the Principal at the school(s).

Covert monitoring

The Trust will not engage in covert surveillance of any type. If such surveillance is requested, for example, by the police for the detection and prevention of crime, specific legal requirements will have to be satisfied, mainly contained in the Regulation of Investigatory Powers Act 2000.

Storage and Retention of CCTV images

- Recorded data will not be retained for longer than is necessary. While retained, the integrity of the recordings will be maintained to ensure their evidential value and to protect the rights of the people whose images have been recorded.
- Data will be stored on the CCTV servers for up to 30 days. Footage may be overwritten before this time depending on automated storage requirement processes.
- Data which has been exported as evidence must be securely stored and deleted once the footage is no longer required.

Access to CCTV images

- Access to recorded images will be restricted to those staff authorised to view them and will not be made more widely available. Viewing of images or footage must be requested via Senior Leadership, Safeguarding, Premises or IT Technical Teams.
- Other staff are permitted to view the footage for identification purposes and incidents they are involved in, when absolutely necessary.
- Where an incident requires the assistance of a student/pupil to identify another person or explain a situation, every care will be taken to show only what is related to the incident. All viewing must be supervised by a senior member of staff and the student must not have any means of copying the images.
- No CCTV video images may be shared with any parent/guardian, unless the video only contains a child they have direct parental responsibility for. If a video contains other personally identifiable information of any other child, consent must be gained from the child (if over 13) and from their parent/guardian, before footage is viewed. All footage must be viewed with the supervision of a

Principal or a senior leader they nominate. No footage may be shared via any means, either electronically or printed.

Subject Access Requests (SAR)

- Individuals have the right to request access to CCTV footage relating to themselves under the Data Protection Act.
- All requests should be made in writing to the Principal or COO. Individuals submitting requests for access will be asked to provide sufficient information to enable the footage relating to them to be identified. For example, date, time and location.
- The Trust does not have the technology to edit and mask individuals in CCTV video files. If the footage contains personally identifiable information of others, and the requester is not an employee, the Trust has the right to refuse the request.
- The Collegiate reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

Access to and disclosure of images to third parties

- There will be no disclosure of recorded data to third parties other than to authorised personnel such as the Police and service providers to the Trust, where these would reasonably need access to the data.
- Requests should be made in writing to the Principal or COO.
- The data may be used within the school's behaviour, discipline and grievance procedures as required, and will be subject to the usual confidentiality requirements of those procedures.

Complaints

Complaints and enquiries about the operation of CCTV within the Trust should be directed to the Principal or COO in the first instance.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Policy is followed.
Staff must immediately inform the Principal or COO of abuse of this policy.

Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities, significant changes to the organisation or technical infrastructure, changes to any applicable UK legislation. Changes to this policy will be published on the Trust's website.

Relevant laws, including the CCTV Code of Practice (2012), Regulation of Investigatory Powers Act (RIPA) (2000), Data Protection Act (2018), Freedom of Information Act (2000), Human Rights Act (1998), Computer Misuse Act, Copyright, Design & Patents Act and The Telecommunications Act apply to all operators and schools of Trust CCTV Systems at all times.