



CCTV Policy

Approved by: Board of Trustees

Reviewed by: ELT (CH)

Latest Policy review: Spring 2024 – Full Board Meeting – 18th April 2024

Date for Next Policy review: Spring 2026

Summary of changes in this version

(p2) – Inclusion of Legislation and Guidance
(p3) – Statement of intent - amendment to use of CCTV footage
(pp 4-5) – Inclusion of Roles and Responsibilities
(p6) – Removal of covert surveillance clause
(pp 7-9) – Inclusion of Access to CCTV Footage
(p8) – Inclusion of System Upgrades

INTRODUCTION

The YES Trust and its schools use their CCTV systems for a number of reasons. It is used to help protect against crime and also aids in the safety of students, staff, parents, visiting professionals and members of the public whilst on Trust/school premises. The camera systems we use comprises a number of fixed and dome cameras located around the school sites (appendices with school floor plans and approximate location of cameras to be included).

Cameras can be monitored and adjusted from the school office, and headteachers, office managers, and site managers also have access to footage remotely, via a password protected portal. This code of practice follows the Data Protection Act 2018 and UK General Data Protection Regulations (UK GDPR) guidelines and will be subject to bi-annual review.

The CCTV system is owned solely by the Trust, and members of the Trust Executive Leadership team are allowed immediate access to CCTV footage at any of the Trust's premises, at any time.

LEGISLATION AND GUIDANCE

This policy is based on:

Legislation

- [UK General Data Protection Regulation](#)
- [Data Protection Act 2018](#)
- [Human Rights Act 1998](#)
- [European Convention on Human Rights](#)
- [The Regulation of Investigatory Powers Act 2000](#)
- [The Protection of Freedoms Act 2012](#)
- [The Freedom of Information Act 2000](#)
- [The Education \(Pupil Information\) \(England\) Regulations 2005 \(as amended in 2016\)](#)
- [The Freedom of Information and Data Protection \(Appropriate Limit and Fees\) Regulations 2004](#)
- [The School Standards and Framework Act 1998](#)

- [The Children Act 1989](#)
- [The Children Act 2004](#)
- [The Equality Act 2010](#)

Guidance

- [Surveillance Camera Code of Practice \(2021\)](#)

OBJECTIVES OF THE CCTV SYSTEM

- To protect the school buildings and their assets
- To increase personal safety and reduce the fear of crime
- To support high level teaching and learning
- 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, private property, students, staff and visitors
- To assist in managing the school

STATEMENT OF INTENT

The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018 guidelines and the Trust will seek to comply with the requirements both of the Data Protection Act and the Commissioner's Code of Practice.

The Trust will treat the CCTV system and all information, documents and recordings obtained and used as data, which are protected by the act, in the strictest of confidence.

CCTV cameras will be used to monitor activities within the Trust's schools, car parks, other public areas and surrounding grounds to identify criminal activity actually occurring, anticipated, or perceived, for the purpose of securing the safety and well-being of all. Cameras are also used to safeguard staff, pupils and other users of the premises from harm. This might include reviewing footage in instances of bullying or intimidating behaviour, breaches of school rules and regulations or where the headteacher needs to safeguard a child or staff member. The headteacher might also use footage to determine the facts when dealing with accusations/complaints from children, staff or other stakeholders. Wherever possible, within all schools, cameras will be positioned to cover site entrances/exits, car parks and reception/lobby areas. Camera's may also be positioned in dining/social areas and corridors around the school where appropriate, to help safeguard staff and pupils. This is especially important in areas that do not have direct supervision from staff.

Private dwellings and property other than that in the periphery of a view that is centrally focused upon school site locations, will be blanked out from any camera view.

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 from the headteacher (or deputy in their absence), as set out in the Regulation of Investigatory Power Act 2016. Images will only be released to the police for use for the investigation of a specific crime and with the consent of the headteacher (or deputy in their absence).

No images will be released to anyone for the purposes of entertainment. The planning and design of the CCTV layout in schools has endeavoured to ensure that the scheme will give maximum effectiveness and efficiency, but it is not possible to guarantee that the systems will cover or detect every single incident taking place in the areas of coverage.

It is not the intent of the Trust to use CCTV in classrooms. However, if after an appropriate risk assessment has been carried out it is deemed to be necessary by a headteacher / DSL for the safety of staff and pupils, then staff will be consulted, and cameras may be installed. This must be done in consultation with Executive Trust Leaders.

ROLES AND RESPONSIBILITIES

The Board of Trustees

The Board of Trustees has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in Relevant Legislation and Guidance section) is complied with.

The headteacher

The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified
- Ensure that the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO/Trusts Director of Business in the use of the system and in data protection
- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO/Trusts Director of Business and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties

The data protection officer (Judicium Consulting Limited)

The data protection officer (DPO) will:

- Provide training and guidance to staff to recognise a subject access request
- Provide the Trust with support and advice in relation to any Subject Access Requests received
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments

- Act as a point of contact for communications from the Information Commissioner's Office
- Provide advice and support in relation to any requests for third-party access to CCTV footage

OPERATION OF THE SYSTEM

The CCTV will be managed by the Trusts Director of Business and on site by school headteachers, in accordance with the principles and objectives expressed in this policy. The day-to-day management will be the responsibility of the school office manager and site manager during the school day. The control panel will only be used by the Leadership Team. The CCTV systems will be in operation 24 hours a day, every day of the year.

CONTROL OF CAMERAS

The office manager and/or site managers will, on a weekly basis, check that all cameras are functional and the system is recording. Administrative functions will include the maintenance of hard disc space. Visitors and contractors wishing access to the CCTV system or recording system will be subject to the arrangements outlined below.

Authorised users and managers of the CCTV System must satisfy themselves of the identity of anyone who is to have access to the CCTV System and the purpose of the access. Where any doubt exists over the grounds for access, permission will be refused. Emergency procedures will be used in appropriate cases to call the emergency services.

MONITORING AND STORAGE

Information is held on the hard drive of the CCTV unit and is automatically wiped after a set period of time. This period is currently set to a maximum of 30 days. However, regarding any safeguarding incidents or incidents of a criminal nature or, if any information is required for evidence it will be retained in accordance with the Trusts retention policy and any subsequent legal requirements:-

SIGNAGE

Schools using CCTV on their sites must display signage to inform all site users that CCTV is in operation on site. There should be clearly visible signs both externally, near the site entrances, and internally, when people are entering the building.

CD/DVD/RECORDING

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

- Each record must be identified by a unique mark.

- Before using each recording, media must be cleaned of any previous recording.
- The controller shall register the date and time of recorded insert, including the reference.
- A recording required for evidential purposes must be witnessed, signed by the controller, dated and stored in line with the safeguarding or legal requirements by which the evidence has been produced.
- If the record is archived, the reference must be noted. Recording media may be viewed by designated operators and the police for the prevention and detection of crime.

A record will be maintained of the release of records to the police or other authorised applicants.

Requests by the police can only be actioned where there is a legal basis to do so. Should a record be required as evidence, a copy may be released to the police under the procedures described in this policy.

Records will only be released to the police on the clear understanding that the record remains the property of the Trust, and both the record and information contained on it are to be treated in accordance with this code.

The Trust also retains the right to refuse permission for the police to pass on the record or any part of the information contained therein to any other person.

The police may require the Trust to retain the stored records for possible use as evidence in the future. Such records will be properly indexed and securely stored until the police needs them.

Applications received from outside bodies (e.g. solicitors) to view or release records will be referred to the headteacher and data protection officer. A charge may be made to cover the costs of producing the material.

ACCESS TO CCTV FOOTAGE

Access will only be given to authorised persons, for the purpose of pursuing the aims stated in the statement of intent (p3), or if there is a lawful reason to access the footage.

Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log.

Any visual display monitors will be positioned so only authorised personnel will be able to see the footage.

Staff access

The following members of staff have authorisation to access the CCTV footage:

- Trust Executive Leadership team
- The headteacher
- The deputy headteacher
- The data protection officer
- The office manager/site manager

- Anyone with express permission of the headteacher

CCTV footage will only be accessed from authorised personnel's work devices, or from the visual display monitors.

All members of staff who have access will undergo training to ensure proper handling of the system and footage.

Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

Subject access requests (SAR)

The Data Protection Act provides data subjects – those whose image has been captured by the CCTV system and can be identified – with a right to access data held about themselves, included those obtained by CCTV. Requests for such data should be made to the headteacher.

Third-party access

CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in the Objectives of the CCTV System (e.g. assisting the police in investigating a crime).

Footage will only ever be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

All requests for access should be set out in writing and sent to the headteacher and/or the DPO.

The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose and will provide advice to the school about this. The school may seek legal advice if necessary.

The school, with support from the DPO, will ensure that any disclosures that are made are done in compliance with UK GDPR.

All disclosures will be recorded by the school.

SYSTEM UPGRADES

Trust schools follow the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading.

The system is used only for the purpose of fulfilling its aims (stated in Objectives of the CCTV System and Statement of Intent).

When the CCTV system is replaced, developed or upgraded the system will be reviewed to ensure it is still justifiable, necessary and proportionate.

The DPO will provide advice and support in regard to this review.

Those whose privacy is most likely to be affected, including the school community and neighbouring residents, may be consulted during this review, and any appropriate safeguards will be put in place.

A review will be conducted whenever cameras are moved, and/or new cameras are installed.

If any security risks are identified in the course of this review, the school will address them as soon as possible.

BREACHES OF THE CODE (including breaches in security)

Any breach of this policy by school staff will be initially investigated by the headteacher (or appointed senior member of staff), in order for appropriate disciplinary action to be taken. Any serious breach of the Code of Practice will be immediately investigated by the Director of Business, or if appropriate, the headteacher of the school (or appointed senior member of staff) and recommendations made on how to remedy the breach.

COMPLAINTS

Any complaints about the school's CCTV system should be in writing and addressed to the headteacher or, where the complaint is about the headteacher, to the Chair of the Local Support Board (LSB). Complaints will be investigated in accordance with the Complaints Policy.

LINKS TO OTHER POLICIES

- Data protection policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding policy