



Education Learning Trust Multi School Trust

CCTV Policy

Reviewed	Autumn 2025
Next review	Autumn 2028

Revision History

Date	Document Version	Document Revision History	Document Author / Reviser	Document Approver
Sept 2023	1.1	New document	R O'Connell, Director of Finance and Operations	Trust Board 11/10/2023
July 2024	1.2	Revised document	M Guest – Trust Facilities Manager	Trust Board 17/07/2024
October 2025	1.4	Revised document	M Keefe - DPO	Finance, Audit and Risk and Resources 04/12/2025

Contents

1. Introduction	3
2. Purpose of Policy	3
3. Scope	3
4. Policy	3
5. Justification for use of CCTV	4
6. Location of Cameras	5
7. Notification – Signage	5
8. Storage and Retention	5
9. Access	6
10. Responsibilities	7
11. Implementation and Review	8
12. Appendix 1 - Definitions	9
13. Appendix 2 – Data Privacy Impact Assessment (DPIA)	11
14. Appendix 3 - Checklist	13
15. Appendix 4 – Data Subject Access Request	15

1 Introduction

- 1.1 Closed Circuit Television Systems (CCTVS) are installed in Education Learning Trust Secondary Schools. Any new CCTV systems will be introduced in consultation with staff, the SLT (Senior Leadership Team) and the Trust Board. Where systems are already in operation, their operation will be reviewed regularly in consultation with staff, the SLT and Governing Body.

2 Purpose of Policy

- 2.1 The purpose of this policy is to regulate the use of Closed-Circuit Television and its associated technology in the monitoring of both the internal and external environment of the premises under the remit of the Trust.
- 2.2 CCTV systems are installed (both internally and externally) in premises for the purpose of enhancing security of the building and its 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 environment of the premises during both the daylight and night hours each day. CCTV surveillance at the schools is intended for the purposes of:
- protecting the school buildings and School assets, both during and after school hours
 - promoting the health and safety of staff, pupils and visitors
 - preventing bullying and informing decisions following serious incidents
 - reducing the incidence of crime and anti-social behaviour (including theft and vandalism)
 - supporting the Police in a bid to deter and detect crime
 - ensuring that the school rules are respected so that the school can be properly managed
 - supporting safeguarding procedures regarding entry of visitors to the site

3 Scope

- 3.1 This policy relates directly to the location and use of CCTV and the monitoring, recording and subsequent use of such recorded material. Where classes and activities are carried out in school, we will ensure that CCTV systems, where installed, are operated only in a way that is compatible with the provisions of this policy.

4 Policy

- 4.1 The Trust as the corporate body has a statutory responsibility for the protection of its property and equipment as well as providing a sense of security for its employees, pupils, and visitors to any premises.
- 4.2 The Trust owes a duty of care under the provisions of Safety, Health and Welfare at Work Act 2005 and associated legislation and utilises CCTV systems and their associated monitoring and recording equipment as an added mode of security and surveillance for the purpose of enhancing the quality of life of the School

community by integrating the best practices governing the public and private surveillance of its premises.

- 4.3 The use of the CCTV system will be conducted in a professional, ethical, and legal manner and any diversion of the use of CCTV security technologies for other purposes is prohibited by this policy.
- 4.4 Information obtained through the CCTV system may only be released when authorised by the School Headteacher or those who is delegated this duty in their absence. Any requests for CCTV recordings/images from the Police will be fully recorded and legal advice will be sought if any such request is made.
- 4.5 If a law enforcement authority, such as the Police, is seeking a recording for a specific investigation, the Police may require a warrant and accordingly any such request made by the Police should be requested in writing and the school will immediately seek legal advice.
- 4.6 CCTV monitoring of public areas for security purposes will be conducted in a manner consistent with all existing policies adopted by the Trust, including Equality Policy, Code of Conduct, IT Acceptable Use Policy, Exclusions Policy for dealing with complaints of bullying and harassment and other relevant policies, including the provisions set down in equality and other educational and related legislation.
- 4.7 This policy prohibits monitoring based on the characteristics and classifications contained in equality and other related legislation e.g., race, gender, sexual orientation, national origin, disability etc.
- 4.8 Digital format monitoring of public areas for security purposes within School premises is limited to uses that do not violate the individual's reasonable expectation of privacy.
- 4.9 Information obtained in violation of this policy may not be used in a disciplinary proceeding against an employee of the school or a student attending one of its school schools.
- 4.10 All CCTV systems and associated equipment will be required to be compliant with this policy. Recognisable images captured by CCTV systems are "personal data." They are therefore subject to the provisions of the Data Protection Act 2018 and the UK GDPR.

5 Justification for use of CCTV

- 5.1 Chapter 2 (Section 88) of the Data Protection Act 2018 requires that data be "adequate, relevant and not excessive" for the purpose for which it is processed. This means our I Schools need to be able to justify the obtaining and use of personal data by means of a CCTV system.
- 5.2 The use of CCTV to control the perimeter of the school buildings for security purposes has been deemed to be justified by the Trust. The system is intended to capture images of intruders or of individuals damaging property or removing goods without authorisation.

- 5.3 In other areas of the school where CCTV has been installed, e.g. hallways, stairwells, locker areas, the Headteacher has demonstrated that there is a proven risk to security and/or health & safety and that the installation of CCTV is proportionate in addressing such issues that have arisen prior to the installation of the system.

6 Location of Cameras

- 6.1 The location of cameras is a key consideration. Use of CCTV to monitor areas where individuals would have a reasonable expectation of privacy would be difficult to justify. Our schools will select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. Cameras placed to record external areas are positioned in such a way as to prevent or minimise recording of passers-by or of another person's private property.

7 Notification – Signage

- 7.1 The Headteacher will provide a copy of this CCTV Policy on request to staff, students, parents/carers and visitors to the school.
- 7.2 Adequate signage will be placed at each location in which a CCTV camera(s) is sited to indicate that CCTV is in operation. Adequate signage will also be prominently displayed at the entrance to the school property.
- 7.3 Appropriate locations for signage will include:
- at entrances to premises i.e., external doors, school gates.
 - reception area
 - at or close to each internal camera
- 7.4 The CCTV sign should include the following:
- That the area is covered by CCTV surveillance and pictures are recorded
 - The purpose of using CCTV
 - The name of the school
 - The contact telephone number or address for enquiries



8 Storage and Retention

- 8.1 Chapter 2 (Section 90) of the Data Protection Act 2018 states that data "shall not be kept for longer than is necessary for" the purposes for which it is

processed. A data controller needs to be able to justify this retention period. For a normal CCTV security system, it would be difficult to justify retention beyond a month (28 days), except where the images identify an issue – such as a break-in or theft and those particular images/recordings are retained specifically in the context of an investigation/prosecution of that issue.

- 8.2 The images/recordings will be stored in a secure environment with a log of access kept. Access will be restricted to authorised personnel. Supervising the access and maintenance of the CCTV System is the responsibility of the Headteacher. The Headteacher may delegate the administration of the CCTV System to another staff member.
- 8.3 In certain circumstances, the recordings may also be viewed by other individuals in order to achieve the objectives set out above. When CCTV recordings are being viewed, access will be limited to authorised individuals on a need-to-know basis.
- 8.4 Digital storage will be stored in a secure environment with a log of access to the data kept. Access will be restricted to authorised personnel. Similar measures will be employed when using disk storage, with automatic logs of access to the images created.

9 Access

- 9.1 Digital Storage, storing the recorded footage and the monitoring equipment will be securely stored in a restricted area. Unauthorised access to that area will not be permitted at any time. The area will be locked when not occupied by authorised personnel. A log of access to tapes/images will be maintained.
- 9.2 Access to the CCTV system and stored images will be restricted to authorised personnel only. Access will be authorised by the Headteacher.
- 9.3 In relevant circumstances, CCTV footage may be accessed:
 - by the Police where the school is required by law to make a report regarding the commission of a suspected crime
 - following a request by the police when a crime or suspected crime has taken place and/or when it is suspected that illegal/anti-social behaviour is taking place on a school property
 - to the HSE and/or any other statutory body charged with child safeguarding
 - to assist the school in establishing facts in cases of unacceptable student behaviour, in which case, the parents/guardians will be informed
 - to data subjects (or their legal representatives), pursuant to an access request where the time, date and location of the recordings is furnished

to the school

- to individuals (or their legal representatives) subject to a court order
- to the school insurance company where the insurance company requires evidence in order to pursue a claim for damage done to the insured property

9.4 **Requests by the Police:** Information obtained through digital format monitoring will only be released when authorised by the Headteacher following consultation with the Trust. If the Police request CCTV images for a specific investigation, the Police will require a form 0819B or DP1 form and accordingly any such request made by the Police should be made in writing and the school should immediately seek advice from the Data Protection Officer. Where a 0819B form or DP1 is not provided then Appendix 4 must be completed by the requester as evidence of the disclosure.

9.5 **Access requests:** On written request, any person whose image has been recorded has a right to be given a copy of the information recorded which relates to them, provided always that such an image/recording exists i.e. has not been deleted and provided also that an exemption/prohibition does not apply to the release.

9.6 Where the image/recording identifies another individual, those images may only be released where they can be redacted/anonymised so that the other person is not identified or identifiable. To exercise their right of access, a data subject must make an application in writing to the School Headteacher. **The school must respond within 30 days of the request.**

9.7 Access requests can be made to the following: via the DPO for the Trust **dpo@educationlearningtrust.com**

9.8 A person should provide all the necessary information to assist the DPO for the Trust in locating the CCTV recorded data, such as the date, time, and location of the recording. If the image is of such poor quality as not to clearly identify an individual, that image may not be considered to be personal data and may not be handed over by the school.

9.9 In giving a person, a copy of their data, the school may provide a still/series of still pictures, or digital copy with relevant images. However, other images of other individuals will be obscured before the data is released.

10 Responsibilities

10.1 The Headteacher or the designated person will:

- ensure that the use of CCTV systems is implemented in accordance with the policy
- oversee and co-ordinate the use of CCTV monitoring for safety and security purposes within the school

- ensure that all existing CCTV monitoring systems will be evaluated for compliance with this policy
- ensure that the CCTV monitoring at the school is consistent with the highest standards and protection
- review camera locations and be responsible for the release of any information or recorded CCTV materials stored in compliance with this policy
- maintain a record of access (e.g., an access log) to or the release of digital recordings or any material recorded or stored in the system
- ensure that monitoring recorded tapes are not duplicated for release
- ensure that the perimeter of view from fixed location cameras conforms to this policy both internally and externally
- approve the location of temporary cameras to be used during special events that have particular security requirements and ensure their withdrawal following such events.
- Give consideration to both pupils and staff feedback/complaints regarding possible invasion of privacy or confidentiality due to the location of a particular CCTV camera or associated equipment
- ensure that all areas being monitored are not in breach of an enhanced expectation of the privacy of individuals within the school and be mindful that no such infringement is likely to take place
- ensure that external cameras are non-intrusive in terms of their positions and views of neighbouring residential housing
- ensure that monitoring tapes are stored in a secure place with access by authorised personnel only
- ensure that images recorded on digital recordings are stored for a period not longer than 28 days
- ensure that when a zoom facility on a camera is being used, there is a second person present with the operator of the camera to guarantee that there is no unwarranted invasion of privacy
- ensure that camera control is solely to monitor suspicious behaviour, criminal damage etc. and not to monitor individual characteristics
- ensure that camera control is not infringing an individual's reasonable expectation of privacy in public areas
- ensure that where the Police request to set up mobile video equipment for criminal investigations, advice has been obtained from the Data Protection Officer
- perform a periodic assessment of the CCTV system using Appendix 4
- record any access to the system on a CCTV Log to be available for inspection

11 Implementation and Review

- 11.1 The policy will be reviewed and evaluated on a regular basis. On-going reviews and evaluation will take cognisance of changing information or guidelines (e.g., from the Information Commissioner, Police, Department for Education, national management bodies, legislation and feedback from parents/guardians, students, staff, and others.
- 11.2 The date from which the policy will apply is the date of adoption by the FARR Committee. Implementation of the policy will be monitored by the Headteacher and Trust.

12 Appendix 1 - Definitions

Definitions of words/phrases used in relation to the protection of personal data and referred to in the text of the policy.

CCTV – Closed-circuit television is the use of digital format cameras to transmit a signal to a specific place on a limited set of monitors.

The Data Protection Acts – The Data Protection Act 2018, UK GDPR and the Data Use and Access Act 2025 confer rights on individuals as well as responsibilities on those persons handling, processing, managing and controlling personal data. All School staff must comply with the provisions of the Data Protection Acts when collecting and storing personal information.

Data - information in a form that can be processed. It includes automated or electronic data (any information on computer or information recorded with the intention of putting it on computer) and manual data (information that is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system).

Personal Data – Data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller.

Access Request – this is where a person makes a request to the organisation for the disclosure of their personal data under Section 3 and/or section 4 of the Data Protection Acts.

Data Processing - performing any operation or set of operations on data, including:

- Obtaining, recording, or keeping the data,
- Collecting, organising, storing, altering, or adapting the data,
- Retrieving, consulting, or using the data,
- Disclosing the data by transmitting, disseminating, or otherwise making it available,
- Aligning, combining, blocking, erasing, or destroying the data.

Data Subject – an individual who is the subject of personal data.

Data Controller - a person who (either alone or with others) controls the contents and use of personal data.

Data Processor - a person who processes personal information on behalf of a data controller, but does not include an employee of a data controller who processes such data in the course of their employment, for example, this might mean an employee of an organisation to which the data controller out-sources work. The Data Protection Acts place responsibilities on such entities in relation to their processing of the data.

13 Appendix 2 – Data Privacy Impact Assessment (DPIA)

Before the school installs a new CCTV system, it is recommended that a documented DPIA is carried out. A school which properly conducts such an assessment is less likely to introduce a system that contravenes the provisions of the Data Protection Act 2018, UK GDPR and the Data Use and Access Act 2025. This is an important procedure to adopt as contravention may result in action being taken against a School by the Office of the Data Protection Commissioner, or may expose a school to a claim for damages from a student.

Some of the points that might be included in a DPIA are:

- What is the school's purpose for using CCTV images? What are the issues/problems it is meant to address?
- Is the system necessary to address a pressing need, such as staff and student safety or crime prevention?
- Are the CCTV cameras intended to operate on the outside of the premises only?
- Is it justified under the circumstances?
- Is it proportionate to the problem it is designed to deal with?
- Is it intended that CCTV cameras will operate inside of the building?
- Are internal CCTV cameras justified under the circumstances?
- Are internal CCTV cameras proportionate to the problem they are designed to deal with?
- What are the benefits to be gained from its use?
- Can CCTV systems realistically deliver these benefits? Can less privacy-intrusive solutions, such as improved lighting, achieve the same objectives?
- Does the school need images of identifiable individuals, or could the system use other images which are not capable of identifying the individual?
- Will the system being considered deliver the desired benefits now and remain suitable in the future?
- What future demands may arise for wider use of images and how will they be addressed?
- Is the School, the data controller for the entire CCTV system (bearing in mind that some schools under the PPP are managed for operational purposes by management companies, in which case specific legal advice may need to be sought)?
- Where a management company is in place, is the school satisfied that it complies with the Data Protection Acts with regard to the processing of images of staff, pupils and visitors to your School captured on any CCTV systems under its management?
- What are the views of those who will be under CCTV surveillance?
- What could be done to minimise intrusion for those whose images may be captured, particularly if specific concerns have been expressed?
- How have staff, pupils and visitors been assured by the school that they will not be monitored and that the CCTV system will be used only for the stated purposes?
- Does the school's policy on the use of CCTV make it clear that staff (teaching and

- non-teaching) will not be monitored for performance or conduct purposes?
- Have the views of staff & pupils regarding the location of cameras been taken into account?
- Can the location of each internal camera be justified in accordance with the overall purpose for the use of the CCTV system?
- Has appropriate signage been erected at the location of each internal camera indicating that recording is taking place and outlining the purpose of such recording?
- Who will have access to the system and recordings/images?
- What security measures are in place to protect the CCTV system and recordings/images?
- Are those who will have authorised access to the system and recordings/images clear about their responsibilities?
- Are the camera monitors kept out of view of staff, pupils and visitors and is access to the camera monitors restricted to a limited number of staff on a 'need to know' basis?
- Is the room(s) which houses the camera monitors and the CCTV system securely locked when unattended?
- Does the School have a procedure in place to ensure that recordings/images are erased or deleted as soon as the retention period (28 days) has expired?
- Does the School have a procedure in place for handling requests for access to recordings/images?
- Will appropriate notices be in place to ensure that individuals know that they are being monitored?
- Does the School have a data protection policy? Has it been updated to take account of the introduction of a CCTV system?
- Does the School have a procedure in place to manage access requests seeking a copy of images recorded by the CCTV system (within the statutory timeframe of thirty days)?
- Has the right of access been communicated to staff, pupils, and visitors?
- Has the School communicated its policy on the use of CCTV to staff, pupils and visitors and how has this been done?
- How are new pupils and new staff informed of the school's policy on the use of CCTV?

14 Appendix 3 - Checklist

This CCTV system and the images produced by it are controlled by the IT Manager who is responsible for how the system is used under direction from the company's Data Protection Officer. The company notifies the Information Commissioner about the CCTV system, including any modifications of use and/or its purpose (which is a legal requirement of the current Data Protection Act 2018).

Education Learning Trust has considered the need for using CCTV and have decided it is required for the areas stated in para 2.1. It will not be used for other purposes. The trust will conduct regular reviews of our use of CCTV.

	Checked (Date if appropriate)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime, and these can easily be taken from the system when required			
Staff will be consulted about any proposal to install / amend CCTV equipment or its use as appropriate.			
Cameras have been sited so that they provide clear images.			

Cameras have been positioned to avoid capturing the images of persons not visiting the premises.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The company knows how to respond to individuals making requests for copies of their own images. If unsure the data controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

15 **Appendix 4 – Data Subject Access Request**

For the purposes of this request Police are the third party. We ask that the third-party gain consent from the data subject to disclosure of data from the Education Learning Trust in accordance with Police Form 0819B or DP1 in that any special or personal data requested is supplied to the third party as soon as possible. Where such data is collected for crime prevention and it is not necessary by law to gain the data subjects consent, the third party is to annotate this on the request form.

Data Subject's Information	
Name of the Data Subject	
Date of Birth	
Address where Data Subject attended school	
Third Party Information	
Name of the person requesting information on behalf of the Data Subject	
Address of the person requesting information on behalf of the Data Subject	

