CCTV POLICY

Policy Approved: December 2025
Policy Renewal: December 2027

Reviewed by the SLT MAT Board

"The Trustees of the Southport Learning Trust are committed to safeguarding and promoting the welfare of children and young people at every opportunity and expect all staff and volunteers to share this commitment"

Contents

1. Introduction

The purpose of this Policy is to regulate the management, operation and use of the closed-circuit television (CCTV) system at all Trust sites.

The system comprises of several fixed cameras some of which have sound recording capabilities which is not enabled located around the school and Trust sites. All CCTV recorders are password protected, and monitoring is only available to authorised staff.

This Policy follows Data Protection guidelines, including guidance from the Information Commissioner's Office and the Biometrics and Surveillance Camera Commissioner.

The CCTV system is owned by the Trust.

Authorised Staff include:

- Headteacher
- Senior Leadership Team Members from Schools and Trust
- IT Managers
- Premises Managers
- Data Lead.

All authorised users must sign the CCTV operator agreement (see annex three). This document will be kept on file at the relevant location.

2. Purposes of the CCTV Scheme

- To protect the Trust buildings and their assets
- To increase personal safety and reduce the fear of crime
- To support the law enforcement agencies e.g. police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To assist with the safeguarding and supervision of pupils
- To assist with the prevention and identification of bullying and antisocial behaviour

The Trust has identified the following legal bases for processing CCTV footage which will include personal data; UK GDPR Article 6(1)e (public task) and Article 9(2)(g) (substantial public interest) and Data Protection Act 2018 Schedule 1, paragraph 10 (preventing or detecting unlawful acts) and paragraph 36 processing criminal category data for purposes of substantial public interest.

3. Statement of Intent

The Trust will seek to comply with the requirements of the Data Protection Act ("the Act"), the Information Commissioner's Guidance on Video Surveillance and the Biometrics and Surveillance Camera Commissioner 'Surveillance Camera Code of Practice'.

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

Cameras will be used to monitor activities within the Trust to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of members of the Trust community and members of the public.

Materials or knowledge obtained 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 law enforcement agencies e.g. police. Recordings will never be released to the media for purposes of entertainment.

The planning and design has 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.

Cameras will not record any private premises.

Signs that inform people of the existence of CCTV, as required by UK GDPR and guidance from the Information Commissioner have been placed at access routes to areas covered by the Trust CCTV.

A log is kept of Authorised Staff access to Recorded Images (template below).

4. Operation of and Access to the System

To ensure that administered and managed, in accordance with the principles and objectives expressed in this policy, is the responsibility of the Headteacher.

Images only can be accessed by authorised users via a secure office on a password protected computer onsite. Remote access to the system is not allowed under any circumstances.

Live feeds are available from the CCTV recorder control console. Live feeds are available to authorised staff for the management of the school and Trust sites as well as security of the site and safety of staff and pupils.

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

CCTV recordings will be available for a maximum 30 days unless copied to removable media (CDs, DVDs or tapes etc). After this time any recordings will be automatically overwritten. Where CCTV is copied to be retained for longer periods this will be documented and justified in the Access Log. In this case, the footage will be held in accordance with the Trust Retention Schedule.

5. Printed and Recording Media Procedures

In the event of an incident requiring footage from the system to be retrieved and stored the following procedure will be followed:

- The details of the incident will be passed to an authorised user who will then authorise the use of the system by relevant staff.
- The relevant footage will be identified.
- An entry shall be made on the Recorded Image Viewing Log.
- If the footage is required for investigation, then the User will produce a copy. The Date and Time of the recorded extract will be registered and stored in a secure place.
- The footage may only be viewed by Authorised Staff or relevant staff that have been approved by authorised staff.
- A record of all viewings shall be made, which if required as evidence, may be released to law enforcement agencies e.g. police via an agreed secure data transfer. (Please see DPO police guidance).
- Applications received from outside bodies or Subject Access Requests to view or release records will be notified to the Data Lead.

6. Assessment of the System

The Premises Manager will check and confirm the screen, and cameras are working monthly.

Regular reviews of the system's operation will take place and any necessary changes in procedure and camera sighting/position will be implemented.

The Premises Manager will carry out an annual review of the use of CCTV, using the Annual Review Checklist below and send to the DPO for review.

The Trust will carry out a Data Protection Impact Assessment to review the use of CCTV whenever there is any significant change to the use of the system or the purpose for which is it used, it is the school's responsibility to notify the Trust Data Manager of these changes.

If out of hours emergency maintenance arises, the Headteacher, Premises Manager or Trust Estates Manager will be satisfied of the identity and purpose of contractors before allowing entry.

7. Breaches of the Policy (including breaches of security)

Any breach of this Policy by Trust staff will be initially investigated by the Headteacher, for them to take the appropriate disciplinary action.

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

8. Complaints

Any complaints about the Trust's CCTV systems will be addressed initially to the Headteacher and escalated if necessary.

Complaints will be investigated in accordance with Trust's Complaints Policy/Procedure.

9. Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to access copies of data held about themselves, including those obtained by CCTV.

Requests for Data Subject Access will be made in accordance with the Subject Access Request Procedure.

1. Annexe 1: CCTV System Annual Review Form (example)

CCTV System Annual Review Form			
Name of School/Trust:			
Name of person completing the review:		**Job title:**	
Signed:		**Date of CCTV review:**	

Review Record	Satisfactory		Problems Identified?	Corrective Action Required / Additional Notes *(if relevant)*
	Yes (✓)	No (×)		
The Trust is registered with the Information Commissioner's Office and the next renewal date recorded.				
There is a named individual who is responsible for operation of the system.				
The problem we are trying to address has been clearly defined and installing cameras is the best solution.				
The CCTV system is addressing the needs and delivering the benefits that justified its use.				
The nature of processing or surveillance equipment has not changed since the last review.				
Clear procedures and policies are in place for CCTV and are up to date with any changes to the system/processing (eg CCTV Policy, CCTV DPIA, Privacy Notices).				
The system equipment produces clear images which law enforcement agencies e.g. police can use to investigate crime and these can easily be taken from the system when required.				

Review Record	Satisfactory		Problems Identified?	Corrective Action Required / Additional Notes *(if relevant)*
	Yes (✓)	No (×)		
Cameras have been sited so that they provide clear images.				
Cameras have been positioned to avoid capturing images of people who are not visiting the premises.				
There is sufficient suitable signage notifying people that CCTV monitoring is in operation, including our contact details where it might not be obvious that the system is managed by this school.				
There is sufficient suitable signage notifying people that CCTV monitoring is in operation, including our contact details where it might not be obvious that the system is managed by this school.				
Information is available to help deal with queries about operation of the system and how individuals can make access requests.				
Sufficient safeguards are in place to protect wireless transmission systems from interception.				
There are sufficient controls and safeguards in place if the system is connected to, or made available across, a computer, e.g. an intranet.				
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.				
A log is maintained of all access to the system, including names of staff viewing images and whether any images are shared.				
Recorded data 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, but no longer than 30 days.				
The process for deleting data is effective and being adhered to.				
Except under the direction of an appropriate public authority (usually police), images will not be provided to				

Review Record	Satisfactory		Problems Identified?	Corrective Action Required / Additional Notes *(if relevant)*
	Yes (✓)	No (×)		
third parties, unless the Headteacher has approved the disclosure of the data under the advice of the DPO.				
When information is disclosed, it is transmitted as securely as possible e.g. viewed on school premises, hand delivered/collected in person on an encrypted device, a fully tracked postal service etc.				
Authorised users are trained in security procedures and there are sanctions in place for any misuse of surveillance system information.				
Regular checks are carried out to ensure that the system is working properly and produces high quality and useful data.				
There is adequate protection against any cyber security risks or risks in the event of any hardware being lost/stolen.				
There is a system in place to ensure that any manufacturer recommended CCTV system and equipment updates, especially of security software are regularly sought, applied and checked as properly functioning.				

2. Annexe 2: CCTV Recorded Image Access Log (example)

CCTV Recorded Image Access Log					
Name of School/Trust:					
Authorised member of staff *(name)*	Camera Number / Location	Date & Time of Recording	Reason for viewing *(eg vandalism, behaviour incident)*	Further action taken *(eg any images / recordings saved / shared?)*	Notes *(eg authorisation for sharing / retention period for retained images*

CCTV Recorded Image Access Log

Name of School/Trust:					
Authorised member of staff *(name)*	Camera Number / Location	Date & Time of Recording	Reason for viewing *(eg vandalism, behaviour incident)*	Further action taken *(eg any images / recordings saved / shared?)*	Notes *(eg authorisation for sharing / retention period for retained images*

CCTV Operator Agreement

People authorised to view the recordings are set out in the CCTV Policy.

I confirm I have read and understood the CCTV Policy and agree to adhere by the rules of the policy as an operator of this system.

In addition, I will update the CCTV Recorded Image Access Log each time I access the system to review a recording. I will:

- record the reason for viewing any images
- detail any retained images, why these were retained and diarise to review saved images for deletion
- I will ensure any retained images are password protected.
- I understand images including retained images must not be shared with third parties, including staff who are not part of the senior leadership team.

Any shared images must have approval for sharing from the Headteacher.

Agreement

Authorised operator (name):	
Signature:	
Date:	
I confirm that the above-named person is an authorised operator of the CCTV system.	
Headteacher (name):	
Signature:	
Date:	

Annex 4: How to Guide for Police Requests

A law enforcement authority can ask you to share personal data with them. For schools this is most commonly the Police, therefore this guide focuses on how to deal with requests from the Police.

The Police must clearly explain what personal data they require and why they need it using the appropriate form (this varies between each constabulary). While the forms may have different names or reference numbers, the content of what it must include is set by the National Police Chiefs' Council.

In some cases, the Police may have obtained the consent of the data subject for you to share this information, in this case you must ensure that you deem the consent appropriate. However, in most cases the Police deem that it is not appropriate to inform the data subject of the request as it would be likely to prejudice the enquiry.

The Police must justify why the information requested is necessary and proportionate to their enquiry, it is therefore not the school's responsibility to determine what is relevant to their enquiry. The school must provide all information that has been asked for so long as it has been appropriately redacted, and the school has a lawful basis for sharing (in most cases this is public interest).

The DPO (Data Protection Officer) team will assist client schools to identify, categorise and deal with requests for information.

Detailed and regular communication between the school and the DPO will be needed during the process -this guide is designed to supplement the DPO's advice.

Remember there are Bitesize sessions to support you too: Bite-sized workshops

	Process	Notes
1.	**Receive request**	The request must be from an official police email address, if you are concerned around the identity of the officer, you can carry out an officer identity check by calling 101. If the police officer requires the information in response to an emergency, you may share this information under the vital interest lawful basis. In all other circumstances you should receive a Third-Party Material Request Form (depending on the constabulary, the name may vary). The DPO will advise you if they have sent the appropriate form. If you have not received the correct form or the request has been made verbally/in person, then you must ask them to send you a Third-Party Material Request Form before you can proceed with the request. An example of a Third-Party Material Request Form and what details it should include can be found on GDPRiS.
2.	**Log on GDPRis**	Add the request to GDPRiS as a 'Data Sharing' request and add all relevant information. Scope: add the actual wording of the request if possible. Response date: on the request form the Police should have identified when they need the data by. If not, this must be dealt with as quickly as possible. See 'How to Log and close an Information Request on GDPRis' guide (Link can be found on the front page of the Information Requests Overview Guide').
3.	**Send request form to DP Team**	Send the Request Form to the DPO team (dpforschools@derbyshire.gov.uk). The DPO will check that the form has been completed correctly and advise how to proceed.

4.	**Collate data**	Search for and collate all data that has been asked for. Review the data in school to ascertain whether there is any data that you shouldn't share with the police, e.g. details of other children that are clearly not relevant. If the data needs redacting before release send it through to the DPO for redaction. Please DO NOT REDACT before sending it to us.
5.	**Send data to DPO** ***{Skip to 7. If no redaction necessary)***	Use a secure method to send the data to us at dpforschools@derbyshire.gov.uk, this could be: • Secure Email • Encrypted email • Egress • Sharepoint • Cryptshare Check with your IT provider if you are unsure about the security of your method to transfer the data.
6.	**Review the Redacted data**	The DPO will redact the data however it is your responsibility to review the redactions prior to release to ensure that you are happy and agree with all redactions. At this stage, if necessary, you can request any further redactions.
7.	**Send materials to the Police**	Send the data to the police as per their instructions, this could be: • Hard copy- make sure they sign for the release, scan this and save appropriately. • Email- ensure to send this securely and add read or delivery receipt and save appropriately. If releasing the data by email, ensure that the receiving address is an official police email address.
8.	**Audit trail of decision making**	You must keep an audit trail of your decision making, including your lawful basis for sharing. This can either be on GDPRiS in the comments or you can use the template form which can be found on GDPRiS in the documents section. Please contact the DP Team if you need help completing this.
9.	**Close**	Close the log on GDPRis (see *'How to Log and Close an Information request on GDPRis')* and ensure any copies of emails, correspondence and documents are saved in accordance with the school's retention of the pupil record policy. *The DPO service will retain their copy of materials and communication for a minimum period of 2 years from closure providing we have not had any further communication.*

Annex 5: Police Request Audit Trail Form

Third Party Response	
☐	We do not hold the requested information
☐	We hold some/ all the requested information and: *(select one)* ☐ We are disclosing all of it ☐ We are disclosing some of it ☐ We are disclosing none of it ☐ Other. Please specify: .....
The Individual **(Choose an item)**	
Description of material to be disclosed (if any)	
Include the date parameters of any material held.	
Reasons for not disclosing all or part of the personal data	
Include, if relevant, what additional information may help you reconsider the request.	
The personal data will be provided	
☐ to view at our location ☐ by you collecting a copy in person Address:	☐ by secure email ☐ by post (signed for delivery)
☐ by another method. Describe:	
Additional comments	
Describe if there is data not specifically requested, but which may be appropriate to disclose based on the context of the request, or anything else you wish to add. Please provide a rationale for any data provided.	

Third Party Lawful basis for the disclosure

Personal Data - the disclosure is lawful because the following apply:

- □ Necessary for compliance with a legal obligation to which the controller is subject; **Article 6(1)(c)** of the Data Protection Act 2018
- □ The data subject has given consent to the processing of his or her personal data for one or more specific purposes **Article 6(1)(a)** of the Data Protection Act 2018
- □ Necessary in order to protect the vital interests of the data subject or of another natural person. **Article 6(1)(d)** of the Data Protection Act 2018
- □ Necessary for a task carried out in the public interest - **Article 6(1)(e)** of the Data Protection Act 2018
- □ Necessary for the legitimate interests pursued by the data controller or another third party (the **police**)-**Article 6(1)(f)** of the Data Protection Act 2018

Special Category Data - the disclosure is:

- □ None to be disclosed
- □ Necessary for reasons of substantial public interest and on the basis of law - Article 9(2)(g) of the Data Protection Act 2018
- □ Other. Please specify: .....

and we meet the DPA 2018 Schedule 1 Part 2 condition of:

- ☐ Preventing or detecting unlawful acts
- ☐ Preventing fraud
- ☐ Suspicion of terrorist financing and money laundering
- ☐ Safeguarding of children and individuals at risk

Criminal Data - this disclosure is:

- ☐ None to be disclosed
- ☐ Extension of conditions in Part 2 of this Schedule referring to substantial public interest. This condition is met if the processing would meet a condition in Part 2 of this Schedule but for an express requirement for the processing to be necessary for reasons of substantial public interest.

☐ We **meet one of the DPA 2018 Schedule 1: Part 2 conditions** for the disclosure (which do not require a substantial public interest when used for criminal offence data processing) * *(select one)*

- ☐ **preventing or detecting unlawful acts***
- ☐ **preventing fraud***
- ☐ **suspicion of terrorist financing and money laundering***
- ☐ **safeguarding** of children and individuals at risk*

other* *(if relying on a different condition then* seek *guidance from your Data Protection Officer and/or legal services):* Enter details of DPA 2018 Schedule 1: Part 2 condition met

other* *(if relying on a different condition then* seek *guidance from your Data Protection Officer and/or legal services):* Enter details of which additional condition applies

Name	
Contact Number	
Contact Email	
Date of completion	