

2026

CCTV System Policy



**SOUTHCHURCH
HIGH SCHOOL**



Review Framework

The policy should be reviewed every three years

	Date
This policy was created in:	June 2017
This issue was revised and released in:	December 2024
It was ratified by the Governing Body in:	November 2025
It was amended in:	September 2026
It will be reviewed in:	November 2028



Contents

Page number

1. Introduction	3
2. Objectives of the system	3
3. Statement of intent	3
4. System management	4
5. Download media procedures	4
6. Assessment of the system and code of practice	5
7. Complaints	5
8. Access by the data subject	5
9. Breaches of the policy	5
10. Public information	5
11. Summary of key points	5
Appendix 1	
Request to View CCTV Footage	7
Appendix 2	
User Access and Confidentiality Agreement	8



1. Introduction

- 1.1. The purpose of this Policy is to regulate the management, operation and use of the CCTV system (Closed Circuit Television) at Southchurch High School, hereafter referred to as 'the school'.
- 1.2. The system comprises of fixed and dome cameras located in and around the school site. All cameras are monitored from the ICT Support Office and images are only available to selected senior staff.
- 1.3. Cameras will only be used to monitor "live" activities within the school and its grounds where criminal activity is actually occurring, anticipated, or perceived, and only with the Headteacher's authority.
- 1.4. Staff may request to view images in support of investigation of incidents at the school. Requests must be made on the form at the end of this policy. All requests must be authorised by the Headteacher or in her absence a Deputy Headteacher.
- 1.5. Authority to view must be gained before viewing images, authority will not be granted retrospectively and viewing images without authority may be treated as data breach.
- 1.6. This Policy follows Data Protection Act guidelines.
- 1.7. The School Policy will be subject to review every three years to include consultation as appropriate with interested parties.

2. Objectives of the CCTV System

- 2.1. To protect pupils, staff and visitors.
- 2.2. To increase personal safety and reduce the fear of crime.
- 2.3. To protect the school buildings and assets.
- 2.4. Without prejudice, to protect the personal property of pupils, staff and visitors.
- 2.5. To support the police in preventing and detecting crime.
- 2.6. To assist in identifying, apprehending and prosecuting offenders.
- 2.7. To assist in managing the school.

3. Statement of Intent

- 3.1. The CCTV system will seek to comply with the requirements both of the Data Protection Act and the Information Commissioner's Code of Practice.
- 3.2. The school will treat the system, all information, documents and recordings (both those obtained and those subsequently used) as data protected under the Act.
- 3.3. Cameras will only be used to monitor "live" activities within the school and its grounds where criminal activity is actually occurring, anticipated, or perceived, and only with the Headteacher's authority.
- 3.4. Cameras will not be used to monitor staff, visitor or student activity. The system will be used for the purpose of securing the safety and wellbeing of the students, staff and school together with its visitors.
- 3.5. The system has been designed to deny observation on adjacent private homes, gardens and other areas of private property.
- 3.6. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose.
- 3.7. Images will only be released to the media for use in the investigation of a specific crime with the written authority of the police.
- 3.8. Images will never be released to the media for purposes of entertainment.
- 3.9. The planning and design have endeavoured to ensure that the system 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.
- 3.10. Warning signs, as required by the Code of Practice of the Information Commissioner will be clearly visible on the site.



System Management

- 3.11. The system will be administered and managed by the Headteacher who will act as the Data Controller, in accordance with the principles and objectives expressed in the policy.
- 3.12. The day-to-day management will be the responsibility of both the Headteacher and the ICT Network Manager who will act as the System Manager.
- 3.13. The system and the data collected will only be available to the Headteacher and the System Manager.
- 3.14. The CCTV system will operate 24 hours each day, every day of the year.
- 3.15. The System 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.
- 3.16. Unless an immediate response to events is required, cameras will not be directed at an individual, their property or a specific group of individuals, without authorisation in accordance with the Regulation of Investigatory Power Act 2000.
- 3.17. The System Manager must satisfy himself of the identity of any person wishing to view images or access the system and the legitimacy of the request. Where any doubt exists access will be refused.
- 3.18. Details of **ALL** visits and visitors will be recorded in the system log book including time/date of access and details of images viewed.
- 3.19. Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- 3.20. The following members of staff have unrestricted access to the CCTV system authorised by the Headteacher:
 - Headteacher
 - Executive Deputy Headteacher
 - Deputy Headteacher
 - Director of Finance and Resources
 - Assistant Headteachers (Behaviour)
 - HoY 7
 - ICT Network Manager
 - Site Team
 - Main Office & Reception Staff (restricted to external entrances)
 - Schools+ (Lettings Security)
- 3.21. All authorised users will sign the User Access and Confidentiality Agreement at Appendix 2 to this policy. The completed agreement will be countersigned by the Headteacher and a copy held on the individual's personnel file.

4. Download Media Procedures

- 4.1. In order to maintain and preserve the integrity of the data (and to ensure their admissibility in any legal proceedings) any download media used to record events from the hard drive must be prepared in accordance with the following procedures: -
 - 4.1.1. Each download media must be identified by a unique mark.
 - 4.1.2. Before use, each download media must be cleaned of any previous recording.
 - 4.1.3. The System Manager will register the date and time of download media insertion, including its reference.
 - 4.1.4. Download media required for evidential purposes must be sealed, witnessed and signed by the System Manager and stored securely.
 - 4.1.5. If download media is archived the reference must be noted.



- 4.2. Images may be viewed by the police for the prevention and detection of crime.
- 4.3. A record will be maintained of the release of any download media to the police or other authorised applicants.
- 4.4. Viewing of images by the police must be recorded in writing.
- 4.5. Should images be required as evidence, a copy may be released to the police under the procedures described in this policy. Images will only be released to the police on the clear understanding that the download media (and any images contained thereon) remains the property of the school, and download media (and any images contained thereon) are to be treated in accordance with Data Protection legislation. The school also retains the right to refuse permission for the police to pass the images on to a third party.
- 4.6. The police may require the school to retain the downloaded media for possible use as evidence in the future. Such downloaded media will be properly indexed and securely stored until they are needed by the police.
- 4.7. Applications received from outside bodies (e.g. solicitors) to view or release images will be referred to the School's legal advisors.
- 4.8. In line with current Government advice, downloaded CCTV footage should be deleted after 30 days. This may be extended if the footage forms part of an ongoing investigation. Footage should be deleted once the investigation is complete but typically within 90 days of the incident.

5. Assessment of the System and Code of Practice

- 5.1. Performance monitoring, including random operating checks, may be carried out by the Headteacher or the Trust Data Controller.

6. Complaints

- 6.1. Any complaints in relation to the school's CCTV system should be addressed to the Headteacher.

7. Access by the Data Subject

- 7.1. The Data Protection Act provides Data Subjects (individuals to whom "personal data" relates) with a right to data held about themselves, including those obtained by CCTV.
- 7.2. Requests for Data Subject Access should be made to the Headteacher abiding to the published policy.

8. Breaches of The Policy

- 8.1. Any breach of the Policy by school staff will be initially investigated by a member of the Senior Leadership Team, appointed by the Headteacher, with a view to taking appropriate action as necessary.
- 8.2. Any serious breach of the Policy involving misuse of the system will be immediately reported to the Headteacher who will decide whether the incident should be reported to the police.

9. Public Information

- 9.1. Copies of this policy will be available to the public, on request, from the school office.

10. Summary of Key Points

- 10.1. This Policy will be reviewed every three years.
- 10.2. The CCTV system is owned and operated by Southchurch High School.
- 10.3. The CCTV system and images are not available to visitors except under circumstances as outlined in this policy.
- 10.4. Liaison meetings may be held with the police and other bodies if required.
- 10.5. Downloaded media will be used properly indexed, stored and destroyed after appropriate use, in accordance with the Data Protection Act.



- 10.6. Images may only be viewed by authorised School staff and the police.
- 10.7. Downloaded media required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- 10.8. Downloaded media will not be made available to the media for commercial or entertainment purposes.



Request to View CCTV Footage

Name of MOS Requesting Access		Date of Request	
Date of Incident	Approximate time of incident	Area/Camera(s)	
Reason for Request			
Signature of Requester			
Request granted/denied*		Brief reason for denial	
Signature of Headteacher		Date	

This request must be signed by the Headteacher (or Deputy in the Headteacher's absence). CCTV footage must only be viewed by those authorised on this form.



Southchurch High School CCTV System – User Access and Confidentiality Agreement

Applies to: All staff authorised to access the School's CCTV system

1. Purpose

This Agreement sets out the conditions under which an authorised user may access, view, search, retrieve, copy or otherwise interact with the Southchurch High School ("the school") CCTV system.

The CCTV system is operated for legitimate school purposes, including the protection of students, staff, visitors and property; the prevention and investigation of crime and misconduct; safeguarding; health and safety; and the investigation of incidents, in accordance with the school's CCTV Policy and applicable law.

Access to CCTV footage is a position of trust and is permitted only where there is a legitimate and authorised reason.

2. Authorised Access

I understand and agree that:

- I may access the CCTV system only where I have been expressly authorised by the school.
- My access rights are personal to me and must not be shared, transferred or disclosed to another person.
- I will use only the account, credentials or equipment allocated to me.
- I will keep all passwords and authentication information secure and confidential.
- I will not attempt to access cameras, recordings, systems or information beyond the level of access granted to me.
- I will not attempt to circumvent, disable or interfere with CCTV security controls, audit logs or other technical safeguards.
- I will immediately report any suspected unauthorised access, lost credentials, security weakness, accidental disclosure or other CCTV-related security incident to the Director of Finance and Resources in his capacity of Data Protection Lead.

3. Acceptable Use

I agree that CCTV footage will be accessed or used only for a legitimate and authorised school purpose.

I will not:

- view CCTV footage out of curiosity or for personal interest;
- access footage relating to myself, colleagues, students, families or other individuals unless specifically authorised for a legitimate purpose;
- use CCTV footage for entertainment, personal investigation, gossip or any other unauthorised purpose;
- photograph, film, screenshot, download, copy or otherwise reproduce footage unless expressly authorised;
- disclose footage or information obtained from the CCTV system to unauthorised persons;
- post, transmit or upload CCTV footage or still images to social media, messaging services, websites or other platforms;
- use CCTV footage to harass, embarrass, threaten or disadvantage any individual;



- alter, manipulate, delete or conceal CCTV footage or associated records;
- use the CCTV system for any purpose that is unlawful or inconsistent with school policy.

4. Confidentiality

I acknowledge that CCTV footage and information obtained through the CCTV system may contain confidential and personal information concerning students, staff, parents/carers, visitors and other individuals.

I therefore agree to keep all such information strictly confidential.

I will not, during or after my employment, engagement or authorisation by the school, disclose, discuss, copy, distribute or otherwise make available CCTV footage or information derived from it to any person who is not authorised to receive it, except:

- where disclosure is expressly authorised by the school;
- where disclosure is necessary for a legitimate school purpose and is permitted under applicable law;
- where disclosure is required by law, a court, law-enforcement authority or another competent authority;
- where disclosure is otherwise permitted under the school's policies and applicable data-protection requirements; or
- where I am uncertain whether disclosure is permitted, I will seek advice from the appropriate school authority before making the disclosure.

This confidentiality obligation continues after my CCTV access has ended and after my employment or other relationship with the school has ceased.

5. Data Protection

I understand that CCTV recordings may constitute personal data and that my access to the system must comply with applicable data-protection legislation and the school's relevant policies and procedures.

I agree to:

- access personal data only where necessary for an authorised purpose;
- process information only in accordance with my role and instructions from the school;
- maintain the security and confidentiality of personal data;
- follow the school's CCTV, data-protection, information-security and records-management procedures;
- comply with applicable retention and deletion arrangements;
- immediately report any suspected personal-data breach or inappropriate disclosure.

6. Safeguarding and Sensitive Material

I recognise that CCTV footage may contain sensitive or distressing material, including incidents involving children or vulnerable individuals.

I will handle such footage with appropriate care, professionalism and discretion and will not access or disclose it unless there is a legitimate and authorised reason.

Where footage may be relevant to a safeguarding concern, criminal investigation or disciplinary matter, I will follow the school's established safeguarding and disciplinary procedures.



7. Disclosure to Third Parties

I will not provide CCTV footage to parents/carers, students, members of staff, members of the public, journalists, social-media users or other third parties unless the disclosure has been appropriately authorised.

Requests for access to CCTV footage or personal data will be referred to the person or team designated by the school to deal with such requests.

Requests from the police or other statutory authorities will be handled in accordance with the school's CCTV Policy.

8. Security and Audit

I understand that use of the CCTV system may be logged or monitored and that the school may audit access to the system.

I accept that the school may review access records to investigate suspected misuse, security incidents, safeguarding concerns, disciplinary matters or compliance with this Agreement.

I will co-operate with any reasonable investigation concerning my use of the CCTV system.

9. Retention and Handling of Copies

I will not retain CCTV footage, still images, recordings or extracts on personal devices, personal cloud storage, removable media or unauthorised systems.

Where a copy of footage is legitimately required for an authorised purpose, I will ensure that it is stored, transferred, retained and securely destroyed in accordance with the school's procedures.

10. Breach of this Agreement

I understand that misuse of the CCTV system or breach of this Agreement may result in:

- withdrawal or restriction of CCTV access;
- investigation under the school's disciplinary procedures;
- safeguarding action where appropriate;
- reporting to relevant authorities where required;
- action under applicable data-protection or other legislation; and/or
- civil or criminal consequences where applicable.

Nothing in this Agreement prevents the school from taking action where it considers that CCTV access has been misused or confidential information has been improperly disclosed.

11. Return and Termination of Access

When my role changes, my authorisation ends, or the school otherwise requires it, I will immediately cease accessing the CCTV system and return or securely dispose of any school equipment, credentials, copies or records in my possession in accordance with school instructions.

My confidentiality obligations will continue after my access has been terminated.



12. Acknowledgement

By signing this Agreement, I confirm that:

- I have read and understood this Agreement;
- I have received or been given access to the school's relevant CCTV and data-protection policies;
- I have read and understood the CCTV Policy;
- I understand the responsibilities associated with CCTV access;
- I understand that CCTV footage and related information must be treated as confidential;
- I will use the CCTV system only for authorised purposes; and
- I will immediately report any suspected misuse, unauthorised disclosure, loss of information or security incident.

Name: _____

Job title / role: _____

Signature: _____

Date: _____

Authorisation

Authorised by: _____

Position: _____

Signature: _____

Date: _____