



CCTV Policy 2026- 2027

DRAFT SUBJECT TO APPROVAL BY COMMITTEE

Document Type:	Colleague Responsible:	Date:	Next Review:
School	Headteacher / DPO	September 2026	September 2027
Approved By Finance, Audit, Risk and H&S Committee			

Updated for the UK data protection framework in force at September 2026

Policy owner	Headteacher / Data Protection Officer
Committee oversight	Finance, Risk, Audit and H&S Academy Committee
Effective date	September 2026
Review cycle	At least annually and sooner where law, guidance, technology or the CCTV system changes
Previous review	May 2026
Related documents	Privacy Notice; Data Protection Policy; Data Retention Schedule; Data Breach Procedure; Safeguarding and Child Protection Policy; Complaints Policy

This policy should be read alongside the School/Trust privacy notice and data protection procedures. Where there is a conflict, applicable law and the School/Trust's current data protection arrangements take precedence.

Equality Statement

Wrotham School strongly promotes equality of opportunity under all circumstances and in all contexts. Please refer to the Trust Equality Policy for further information. The CCTV system will be operated without unlawful discrimination and with due regard to the privacy, dignity and rights of pupils, staff, visitors and contractors.

Contents

1. Aims and statement of intent	4
1.1 Purposes	4
1.2 Prohibited or restricted uses	4
2. Legal and regulatory framework	4
3. Data protection principles and lawful basis	5
3.1 Data protection principles	5
3.2 Lawful basis	5
3.3 Rights and children's information	5
4. Data protection impact assessment and system changes	5
5. Transparency and signage	6
6. Location and positioning of cameras.....	6
6.1 Current locations	6
7. Covert surveillance	6
8. Roles and responsibilities	7
8.1 Trust Board / governing body	7
8.2 Headteacher	7
8.3 Data Protection Officer (DPO)	7
8.4 System Manager	7
9. Operation of the CCTV system	7
10. Storage, retention and deletion	8
11. Access, disclosure and subject access requests	8
11.1 Authorised staff access.....	8
11.2 Third-party disclosure	8
11.3 Subject access requests (SARs)	8
12. Security and personal data breaches	9
13. Complaints and data protection concerns.....	9
14. Monitoring, review and audit	9
Appendix 1 – Current camera locations.....	10
Appendix 2 – CCTV access and disclosure log requirements	10

1. Aims and statement of intent

This policy sets out Wrotham School's approach to the operation, management and use of closed-circuit television (CCTV) and associated surveillance systems on school property.

1.1 Purposes

The CCTV system may be used only for defined, necessary and proportionate purposes, including:

- helping to maintain a safe environment for pupils, staff, visitors and contractors;
- protecting people and property and reducing the risk of crime, vandalism and unauthorised access;
- supporting the prevention and detection of crime and, where appropriate, assisting the police or other lawful investigations;
- investigating accidents, damage to property, incidents and safeguarding concerns where use of CCTV is relevant and lawful;
- supporting the fair investigation of disciplinary, grievance or other internal proceedings where the footage is relevant and its use is lawful; and
- supporting or defending legal proceedings where the footage is relevant.

1.2 Prohibited or restricted uses

- Cameras must not be used for purposes incompatible with those communicated to individuals unless a lawful basis and appropriate transparency assessment support the new purpose.
- Cameras must not be positioned in toilets, changing rooms or other areas where individuals have a heightened expectation of privacy.
- The system must not be used to target or routinely track particular individuals unless this is necessary and proportionate for a specific lawful purpose.
- Audio recording is not permitted. Any proposed change to record or analyse audio requires prior DPO approval, a DPIA and confirmation of a lawful basis before implementation.
- Facial recognition, biometric identification, automated behavioural analysis or other analytics must not be activated without prior DPO approval, a DPIA and a separate assessment of the applicable legal requirements.

CCTV is a supporting control and cannot guarantee that an incident will be captured or that an individual will be identifiable.

2. Legal and regulatory framework

This policy is designed to operate within the law and guidance applicable in England at the date of approval. The principal framework includes:

- UK General Data Protection Regulation (UK GDPR), as amended by the Data (Use and Access) Act 2025 (DUAA);
- Data Protection Act 2018, as amended by the DUAA;
- Data (Use and Access) Act 2025 and relevant commencement provisions;
- Human Rights Act 1998 and the rights protected by the European Convention on Human Rights, as incorporated into UK law;
- Equality Act 2010;
- Protection of Freedoms Act 2012 and the Surveillance Camera Code of Practice (revised 2021), where applicable, and adopted by the School as relevant good practice;
- relevant education, safeguarding, employment and criminal law requirements; and
- current Information Commissioner's Office (ICO) guidance on CCTV/video surveillance, accountability, transparency, security and individual rights.

The Freedom of Information Act 2000 is not the legal basis for responding to a subject access request. CCTV subject access requests are handled under data protection law. Where another information-access regime applies to a particular request, the DPO will advise on the correct process.

3. Data protection principles and lawful basis

CCTV footage of identifiable individuals is personal data. The School will process it in accordance with the UK GDPR and Data Protection Act 2018, as amended by the DUAA.

3.1 Data protection principles

- lawfulness, fairness and transparency;
- purpose limitation;
- data minimisation;
- accuracy, where applicable;
- storage limitation;
- integrity and confidentiality (security); and
- accountability.

3.2 Lawful basis

Before operating, expanding or materially changing the CCTV system, the School will identify and document the lawful basis for each purpose. For the School's public functions, the public task basis may be appropriate where the underlying task or function has a clear basis in law. Legitimate interests may be available for appropriate purposes where the School is not relying on its public tasks and the relevant conditions are met. The DPO will determine and document the appropriate basis for the particular processing.

The School will not rely on consent simply because cameras are in operation. Signage and privacy information are transparency measures; they do not, by themselves, constitute consent.

3.3 Rights and children's information

Pupils and adults have data protection rights in relation to their personal data. Requests involving children will be considered with regard to the child's competence, maturity, rights and best interests, and the authority of any parent or representative seeking access on the child's behalf.

4. Data protection impact assessment and system changes

A Data Protection Impact Assessment (DPIA) will be completed before introducing a new surveillance system or making a change that is likely to result in a high risk to individuals' rights and freedoms. The DPIA will be reviewed where the system, purposes, camera coverage, technology or risks materially change.

- The DPIA will assess necessity, proportionality, privacy impact, lawful basis, transparency, retention, security, access and disclosure arrangements.
- The DPO will be consulted before new cameras are installed, cameras are repositioned, new analytics are enabled, or footage is integrated with another system.
- Expansion or upgrading of the system requires Headteacher approval following DPO advice and consideration of the DPIA.
- Where a supplier or processor handles CCTV footage, the School will ensure appropriate contractual, security and data protection arrangements are in place.

5. Transparency and signage

The School will provide clear information to people before or when they enter areas monitored by CCTV. Signage will be positioned prominently and, where appropriate, repeated within monitored areas.

CCTV signage will identify, as appropriate:

- the School as the operator/data controller (or the correct legal controller under the Trust's governance arrangements);
- the purpose(s) of surveillance;
- a contact point for further information or data protection queries; and
- where to find the fuller privacy information.

The School's privacy notice will provide the fuller information required by data protection law. Where classroom cameras are in use, appropriate signage will be displayed at classroom entrances and the privacy information will clearly explain the monitoring.

6. Location and positioning of cameras

Cameras will be located only where they are necessary and proportionate to achieve the stated purposes. Positioning will be regularly reviewed to minimise unnecessary intrusion and avoid capturing areas outside the School's control unless there is a documented and lawful reason.

Cameras must not be aimed into toilets, changing rooms or private property. Where public areas are incidentally captured, the School will assess whether the field of view can reasonably be reduced without undermining the stated purpose.

6.1 Current locations

- Curve – internal areas and external areas.
- Sports Hall – internal and external areas.
- House – limited internal areas and external areas
- Shearman building – internal areas and external areas
- Oluwale building - internal areas and external areas

The definitive camera map, camera schedule and DPIA are controlled documents and should be maintained by the System Manager/DPO rather than relying on this policy alone for exact camera-by-camera coverage.

7. Covert surveillance

Covert surveillance is exceptional. It will only be considered where there is a specific, documented and lawful reason, such as a serious concern about crime, safeguarding or public safety, and where less intrusive measures are inadequate.

- The DPO must be consulted before covert surveillance is undertaken, except where immediate action is necessary to prevent serious harm, in which case the DPO must be informed as soon as practicable.
- A DPIA or documented equivalent risk assessment will be completed where required.
- The School will consider whether any specific statutory regime applies to the proposed surveillance, including the Regulation of Investigatory Powers Act 2000 where relevant.
- Covert surveillance must be time-limited, targeted and subject to senior approval. It must cease when the purpose no longer justifies it.
- Covert surveillance must not be used simply to avoid normal transparency requirements.

8. Roles and responsibilities

8.1 Trust Board / governing body

- has ultimate oversight of the policy and the lawful governance of the CCTV system;
- ensures adequate resources and accountability arrangements are in place;
- reviews significant risks and any material changes where appropriate.

8.2 Headteacher

- has day-to-day leadership responsibility for the CCTV system;
- works with the DPO to ensure the system remains necessary, proportionate and lawful;
- ensures authorised staff are trained and follow this policy;
- approves system expansion or significant changes following DPO advice and DPIA consideration; and
- decides, with DPO advice, how appropriate third-party disclosure requests should be handled.

8.3 Data Protection Officer (DPO)

- advises on lawful basis, transparency, DPIAs, individual rights, disclosure and data protection risks;
- provides or arranges appropriate training for authorised CCTV users and staff who may receive rights requests;
- monitors compliance and maintains appropriate records;
- advises on and oversees responses to data protection rights requests and complaints;
- acts as a contact point for the ICO and data subjects on CCTV data protection matters;
- checks that retention and deletion arrangements operate as intended; and
- advises on incidents, breaches and any proposed new surveillance technology.

8.4 System Manager

- manages day-to-day operation and maintenance;
- checks for faults and security weaknesses at least termly;
- ensures date/time settings are accurate and checks them at least termly and when clocks change;
- maintains the camera/system inventory and supports the DPO with technical information;
- ensures footage is extracted, stored and deleted securely when authorised; and
- ensures security updates are applied in accordance with the manufacturer's guidance and the School's IT security procedures.

9. Operation of the CCTV system

- The system will operate 24 hours a day, 365 days a year unless temporarily unavailable for maintenance or due to a fault.
- The system will not record audio.
- Recordings will include date and time information.
- Access will be restricted to authorised personnel and will be based on need-to-know.
- Anyone accessing footage must record their name, date/time, purpose and, where relevant, the footage/event accessed.
- Monitors must be positioned so that unauthorised people cannot view live or recorded footage.
- Authorised users must access footage only through approved devices, systems and accounts.
- Users must not photograph, screen-record, copy, download or disclose CCTV footage except where authorised for a legitimate purpose.
- Staff must not use personal devices, personal cloud storage, messaging apps or personal email accounts to store or transmit CCTV footage.

10. Storage, retention and deletion

The standard retention period is 30 days. This is an operational retention period, not a statutory requirement, and will be kept under review against the purposes and risks of the system. The ICO does not prescribe a universal CCTV retention period; retention must be no longer than necessary for the purpose.

- At the end of the standard retention period, footage will be securely overwritten or deleted automatically wherever the system permits.
- Where footage is relevant to an identified incident, complaint, safeguarding matter, disciplinary process, legal claim or law-enforcement investigation, it may be preserved beyond 30 days for as long as necessary. The reason, owner and review/deletion date should be recorded.
- Exported footage will be stored only in an approved secure location. The current operational arrangement is a restricted Microsoft SharePoint directory, subject to Trust IT/security controls.
- Exported footage must be deleted when the purpose for retaining it has ended and it is no longer required for any legal, safeguarding or investigative reason.
- The DPO/System Manager will carry out at least termly checks of retention and deletion controls.

11. Access, disclosure and subject access requests

11.1 Authorised staff access

The following roles are currently authorised to access CCTV footage, subject to training and need-to-know:

- Headteacher – Laura Abbott
- Deputy Head – Victoria Ross
- Acting Headteacher, in the absence of the Headteacher and Deputy Head
- Data Protection Officer – Nigel Newman
- System Manager – Steve Shearman
- any other person expressly authorised by the Headteacher/DPO for a defined purpose.

The named access list must be reviewed whenever personnel change and at least annually.

11.2 Third-party disclosure

CCTV may be disclosed to a third party only where there is a lawful and documented reason. This may include disclosure to police, other lawful authorities, courts, insurers, professional advisers or investigators where necessary and proportionate.

- Requests should normally be made in writing and referred to the Headteacher and DPO.
- The School will disclose only the footage reasonably required for the stated purpose, rather than unrestricted system access.
- Police requests will be handled in accordance with applicable law and the School's data protection and information-sharing procedures.
- All disclosures must be recorded, including the date, recipient, organisation, purpose and footage disclosed.
- Where regular sharing with a processor or other organisation is required, the School will consider whether a data sharing agreement or processor contract is required.

11.3 Subject access requests (SARs)

An individual may request access to personal data contained in CCTV footage. A SAR may be made verbally or in writing and does not need to quote the UK GDPR.

- Staff who receive a request that may be a SAR must refer it to the DPO promptly.
- The School must respond without undue delay and normally within one calendar month. School holidays do not extend this deadline.

- The response period may be extended by up to a further two calendar months where the request is complex or where the individual has made a number of requests. The requester must be informed within the first month if an extension is being used and why.
- The School may ask for reasonable information to confirm identity and locate the footage. The response period may be paused where the ICO's 'stop the clock' rules apply, for example while waiting for necessary clarification or identity information.
- The School will make a reasonable and proportionate search for the relevant footage.
- Where footage includes other identifiable people, the School will consider redaction or other measures to protect their rights. Consent may be considered where appropriate, but disclosure does not automatically depend on obtaining consent.
- A request concerning a child will be handled in accordance with the child's rights, competence, maturity and best interests, and the authority of anyone acting on the child's behalf.
- The School will not refuse a SAR simply because footage is inconvenient to retrieve or because the request is made during a school holiday. Any restriction or refusal must have a lawful basis and be documented.
- In most circumstances no fee will be charged. A reasonable fee may be charged only where permitted by law, for example for manifestly unfounded or excessive requests or additional copies.
- Disclosures will be made securely and records will be retained of the decision and disclosure.

12. Security and personal data breaches

- CCTV systems and footage must be protected by appropriate technical and organisational measures.
- Access credentials must be individual, secure and not shared.
- CCTV equipment, recording devices and storage media must be physically secured.
- Footage should be encrypted in storage and during transfer where technically appropriate.
- Manufacturer security updates and relevant patches must be applied promptly in accordance with the School's IT security procedures.
- Unauthorised access, loss, accidental disclosure, inappropriate sharing, tampering or cyber compromise must be reported immediately under the School/Trust data breach procedure.
- The DPO will assess any suspected personal data breach, including whether notification to the ICO or affected individuals is required.

13. Complaints and data protection concerns

Complaints about the operation of CCTV should normally be made to the Headteacher or DPO and handled under the School/Trust complaints procedure. Where a concern alleges that personal data has been processed unlawfully or in breach of data protection law, it will also be treated as a data protection complaint.

Under the Data (Use and Access) Act 2025, the School must facilitate data protection complaints, acknowledge receipt within 30 days, and take appropriate steps without undue delay to respond and inform the complainant of the outcome. The complainant may also complain to the ICO and may have other legal rights.

The School will keep appropriate records of data protection complaints and use them to identify recurring issues and improve CCTV governance.

14. Monitoring, review and audit

- The continued use of CCTV will be reviewed at least annually to determine whether it remains necessary, proportionate and effective for its stated purposes.
- The review will consider camera positioning, incidents, complaints, SARs, disclosures, retention, security incidents, system performance, equality/privacy impacts and changes in law or ICO guidance.
- The DPO and System Manager will undertake termly operational checks of retention/deletion, access controls, date/time accuracy, system faults and security arrangements.

- Material changes to the system or purposes will trigger a review of the DPIA and privacy information before implementation.
- This policy will be updated sooner where legislation, regulatory guidance, technology or the School's surveillance arrangements materially change.

Appendix 1 – Current camera locations

The policy records the current high-level coverage. The System Manager should maintain a separate controlled camera schedule/map showing camera identifiers, exact locations, field of view, recording status and any privacy masking.

- Curve – internal areas and external areas.
- Sports Hall – internal and external areas.
- House – limited internal areas and external areas
- Shearman building – internal areas and external areas
- Oluwale building - internal areas and external areas

Appendix 2 – CCTV access and disclosure log requirements

The CCTV access/disclosure log should record, as applicable:

- date and time of access;
- name and role of person accessing footage;
- reason/purpose for access;
- camera(s), date/time range or incident reference;
- whether footage was viewed only or exported;
- location and security arrangements for any exported copy;
- recipient and organisation for any disclosure;
- legal/lawful basis or authority for disclosure;
- date footage is due to be deleted/reviewed; and
- authorisation or DPO decision where required.