Olive Academies Independent School

OA-North View

CCTV and Surveillance Policy

Document control table	
Title	CCTV and Surveillance Policy
Date updated and approved	September 2026
Approved by	OAISB
Date of next review	December 2027 (unless legislation necessitates sooner)
Updates/revisions included:	• Independent School Standards (ISS) Alignment: Updated the regulatory framework to explicitly reference compliance with the Education (Independent School Standards) Regulations, with specific emphasis on Part 3 (Welfare, health and safety of pupils) and Part 7 (Complaints). • SEMH Specialism Integration: Embedded specific language ensuring the operation of CCTV is balanced with a trauma-informed, therapeutic environment. This includes explicit restrictions against using cameras to monitor routine behavioural infractions or substituting surveillance for staff-led de-escalation and safe staffing ratios. • Trauma-Informed Access Controls: Restricted the viewing of behavioural incidents and physical interventions to Senior Leadership Team (SLT) members trained in the approved de-escalation and restrictive intervention framework. • Governance and Oversight Enhancement**:** Expanded the review, monitoring, and approval mechanics to mandate formal OAISB sign-off, establishing a

	transparent audit trail for independent school compliance. • External and Multi-Agency Access: Clarified protocols for processing Subject Access Requests (SARs) involving local authority caseworkers, independent child advocates, and the safeguarding masking (blurring) of non-involved pupils. • Standardised Operational Workflows: Standardised the local reporting format and introduced the mandatory Weekly CCTV System Check template to evidence active site-security monitoring.
This policy applies to Olive Academies Independent School OA-North View, herein known as the School and should be implemented consistently throughout the school. Proposed amendments should be referred to the Head of School/Executive Headteacher and OAISB for consideration.	

1. Introduction

At Olive Academies Independent School, we take our responsibility towards the safety of all our staff, visitors, pupils and our extended school communities very seriously. To help protect everyone's safety, we use surveillance cameras to monitor any instances of verbal and physical aggression or physical damage.

The purpose of this policy is to regulate the management, operation and use of the closed-circuit television (CCTV) systems in the school. The systems used in our buildings and premises include a number of fixed, dome and remote cameras located around the school site. The CCTV systems used are owned by Olive Academies. All cameras are monitored via access to secure servers and are only available to approved OA staff (authorised users).

This policy should be read alongside the OA-North View Data Protection Policy and OA-North View Privacy Notices. This policy follows Data Protection guidelines and the Information Commissioners Office CCTV code of practice. This is available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/about-this-guidance/ This policy specifically complies with the Education (Independent School Standards) Regulations, with particular reference to Part 3 (Welfare, health and safety of pupils). In recognition of our status as an SEMH specialist setting, the School ensures that the deployment and operation of CCTV is balanced against our commitment to maintaining a trauma-informed, therapeutic space that minimises pupil anxiety and avoids feelings of hyper-surveillance.

Summary of key points in this policy

- This policy will be reviewed every two years.
- All CCTV systems are owned and operated by Olive Academies.

- The viewing of images and listening to audio is not open to visitors except by prior arrangement and with good reason.
- CCTV recording media will be used properly, indexed, stored and destroyed after appropriate use.
- CCTV recordings may only be viewed by authorised Olive Academies staff and the police.
- CCTV recording media required as evidence will be properly recorded, witnessed and packaged before copies are released to the police.
- CCTV recordings will not be made available to the media for commercial use or entertainment.
- CCTV recording media no longer required will be disposed of securely by incineration or using an approved disposal company which provides certified and secure data destruction.
- Any breaches of this policy will be investigated by the Head of School (HoS). An independent investigation will be carried out for serious breaches.
- Breaches of this policy and remedies will be reported to the HoS and/ or the OA Data Protection Officer.

2. Objectives of OA CCTV systems

The purpose of the CCTV system, such as to:

- To maintain personal safety in our School
- To protect buildings and property
- 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 and private property
- To assist in managing the School

What the CCTV system will not be used for, such as to:

- Encroach on an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- To routinely monitor or manage low-level pupil behaviour that should be handled through standard therapeutic de-escalation strategies.
- To substitute for appropriate staff-to-pupil ratios and active supervision across the school site.

3. Statement of Intent

Any CCTV system in operation in OA premises will be registered with the Information Commissioner under the terms of the Data Protection Act and will seek to comply with the requirements of the Data Protection Act, GDPR and the Commissioner's Code of Practice. OA will treat CCTV systems and all information, documents and recordings obtained and used as data which are protected by the Act.

Cameras will be used to monitor activities within school buildings, car parks and other public areas to

identify criminal activity occurring, anticipated, or perceived, and for the purpose of securing the safety and wellbeing of each school community, together with its visitors.

All staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

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, as set out in the Regulation of Investigatory Power Act 2000.

Materials or knowledge secured 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 the police. Recordings will never be released to the media for purposes of entertainment.

The planning and design has endeavoured to ensure that OA CCTV systems 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.

We do not need to ask individuals' permission to use CCTV, but we make it clear that individuals are being recorded on the premises via the School's Privacy Notices. Security cameras are clearly visible and accompanied by prominent signs (as required by the Code of Practice of the Information Commissioner) explaining that CCTV is in use.

The School does not condone the use of covert surveillance when monitoring OA staff, pupils and/or volunteers. Covert surveillance is any use of surveillance which is intentionally not shared with the subjects it is recording. Subjects are not informed of covert surveillance. Covert surveillance would only be operable in extreme circumstances in line with police protocols and government guidance: https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance

4. Operation of the System

Each OA CCTV system will be administered and managed by the HoS in accordance with the principles and objectives expressed in this policy.

The day-to-day management will be the responsibility of the Senior Leadership Team (SLT) during the day and the Facilities Team out of hours and at weekends.

The main CCTV system will be operated 24 hours each day, every day of the year. Recordings are stored on hard drives for 21 days (with the exception of remote cameras) and are wiped at expiry or retained for investigatory purposes if required.

5. System Functionality & Access

The CCTV System Manager (the facilities manager or in their absence, the HoS) will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional. This check should be recorded on the form here.

Given the specialist SEMH nature of the setting, any review of CCTV footage involving pupil behavioural incidents or physical interventions must be conducted by members of the Senior Leadership Team who hold advanced certification in the trust's approved physical restraint and de-escalation framework. This ensures context-appropriate evaluation of incidents
Access to the CCTV system will be strictly limited to the SLT and the Facilities Team within their designated area of work only.

Unless an immediate response to events is required, authorised staff must not direct cameras at an individual or a specific group of individuals.

Access to the servers (physically or remotely) is limited to the OA HoS, SLT or Facilities Manager via unique accounts which are password protected. Server rooms are secured both during the working day and when not manned.

Other administrative functions will include maintaining recordings and hard disc space, filing and maintaining occurrence and system maintenance logs. Emergency procedures will be used in appropriate cases to call the Emergency Services.

6. CCTV Recording/ Video/ CD / DVD Procedures

To maintain and preserve the integrity of the disks, optical or magnetic media used to record events from the hard drive and the facility to use them in any future proceedings, the following procedure for their use and retention must be strictly adhered to:

- Media required for evidential purposes must be sealed, witnessed, signed by the OA Data Protection Officer or the HoS, dated and stored in a separate, secure, evidence store.
- If media is not copied for the police before it is sealed, a copy may be made later providing that it is then resealed, witnessed, signed by the DPO or HoS, dated and returned to the evidence store.
- Recordings may be viewed by the police for the prevention and detection of crime or for supervisory purposes, authorised demonstration and training.

A record will be maintained of the release of media to the police or other authorised applicants. A CCTV register or logbook will be available at the School for this purpose.

Viewing of recordings by the police must be recorded in writing and in the CCTV register or logbook. Requests by the police can only be actioned under the Data Protection Act.

Media will only be released to the police on the clear understanding that the media remains the property of OA, and both the media and information contained on it are to be treated in accordance with this policy. OA also retains the right to refuse permission for the police to pass to any other person the media or any part of the information contained thereon. On occasions when a court

requires the release of an original recording this will be produced from the secure evidence store, complete in its sealed bag. The police may require OA to retain the stored media for possible use as evidence in the future. Such media will be properly indexed and properly and securely stored until they are needed by the police.

Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the HoS and OA Data Protection Officer. In these circumstances the media will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a Court Order. Should students not related to the incident be visible in footage, steps will be taken to ensure these individuals are not identifiable, e.g. blurred faces in screen shots.

Requests by persons outside OA for viewing or copying disks, or obtaining digital recordings, will be assessed by the HoS and/ or OA Data Protection Officer on a case-by-case basis with close regard to data protection and freedom of information legislation.

The HoS must satisfy themselves over the identity of any visitors who view CCTV images and the purpose of the visit. Where any doubt exists access will be refused. Details of all visits and visitors will be logged and signed off before recordings are viewed. A CCTV register or logbook is held at the School.

Individuals have the right to submit a Subject Access Request to gain access to their personal data in order to verify the lawfulness of the processing. The School will verify the identity of the person making the request before any information is supplied. A copy of the information will be supplied to the individual free of charge; however, OA may impose a 'reasonable fee' (not exceeding the cost of materials) to comply with requests for further copies of the same information.

All requests will be responded to without delay and at the latest, within one month of receipt. In the event of numerous or complex requests, the period of compliance will be extended by a further two months. The individual will be informed of this extension and will receive an explanation of why the extension is necessary, within one month of the receipt of the request.

Where a request is manifestly unfounded or excessive, OA holds the right to refuse to respond to the request. The individual will be informed of this decision and the reasoning behind it, as well as their right to complain to the ICO and to a judicial remedy, within one month of the refusal.

9. Breaches of the OA CCTV Systems Policy (including breaches of security)

Any breach of this policy by OA staff will be initially investigated by the HoS, in order for them to take any appropriate disciplinary action.

The OA Data Protection Officer must be notified of any serious breach of this policy. This will be immediately investigated and an independent investigation carried out to make recommendations on how to remedy the breach.

10. Assessment, Monitoring and Evaluation

The Head of School (HoS) and the Facilities Manager will conduct random operational checks weekly using the *Weekly CCTV System Check* log to ensure hardware compliance and correct camera positioning.

In line with the Independent School Standards, the Senior Leadership Team will conduct a termly review of the CCTV logbook. This review will analyse how often footage was viewed, by whom, and whether the systems are being used proportionally and ethically within our trauma-informed framework.

Annual impact monitoring will take place to ensure that the presence of surveillance does not negatively impact the therapeutic environment or cause heightened anxiety among our SEMH pupil cohort.

11. Complaints

Any complaints regarding the operation of the CCTV system should be directed to the HoS in the first instance. If the issue is not resolved informally, it will be handled in strict accordance with the Olive Academies Complaints Policy, which fulfils the requirements of Part 7 of the Independent School Standards.

12. Access by the Data Subject

The Data Protection Act provides Data Subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV. Requests for Data Subject Access should be made to the HoS.

13. Public Information

Copies of this policy will be available to the public from the School office and will be published on the School's website.

14. Policy Review and Approval

This policy is reviewed every two years by the Head of Facilities and Infrastructure/the Data Protection Officer to ensure compliance with the latest ICO guidance and independent school regulations.

Material changes to the deployment of cameras, or any introduction of new surveillance technology, will trigger an immediate review and an updated Data Protection Impact Assessment (DPIA).

This policy was formally reviewed and approved for use across the School by the **OAISB.**

Weekly CCTV System Check

This checklist supports safeguarding compliance, data protection expectations, and site-security monitoring.

Site: _____ Week Commencing: _____

Completed By (Name & Role): _____

Signature: _____ Date Completed: _____

Section 1 – Camera Functionality

Check	Yes/No	Notes / Actions Required
All cameras operational (no blank screens).	☐ Yes ☐ No	
Lenses clean and unobstructed.	☐ Yes ☐ No	
Night-vision functioning.	☐ Yes ☐ No	
Correct camera positioning; not tampered.	☐ Yes ☐ No	
No damage or vandalism visible.	☐ Yes ☐ No	

Section 2 – Recording & Playback

Check	Yes/No	Notes / Actions Required
System recording continuously.	☐ Yes ☐ No	
Playback works without error.	☐ Yes ☐ No	
Time/date stamps accurate.	☐ Yes ☐ No	
Adequate storage capacity.	☐ Yes ☐ No	

Section 3 – Hardware & Software

Check	Yes/No	Notes / Actions Required
DVR/NVR powered with no warnings.	☐ Yes ☐ No	
Stable network connection.	☐ Yes ☐ No	
Other noteworthy points:		