

Shaw Education Trust

CCTV Policy

Date reviewed: 19th October 2026
Approved by: Peter Cade
Date to be reviewed: 19th October 2029 (or sooner if required, following approval)

1. Introduction

1.1 This policy must be read in conjunction with the Shaw Education Trust's CCTV policy.

1.2 Ivy House School uses closed circuit television (CCTV) images to reduce crime and monitor the school buildings in order to provide a safe and secure environment for pupils, staff and visitors, and to prevent loss or damage to school property.

1.3 The CCTV system comprises fixed cameras located at Main Reception, the Pool Entrance, the Hydro Pool area, and The Vine Building. The additional cameras in the Vine Building are located at: Main Entrance; Play Area towards Library; Air Lock Gates; Rear Right towards Car Park; Side towards School; Rear Left towards Front of School; Internal Main Entrance; Corridor towards Opal Class; Sensory Room Entrance; Outside Moonstones Class; Middle Corridor towards Moonstones.

1.4 The system has sound-recording capability. Audio recording is particularly intrusive and must be disabled by default unless the school has documented a specific, necessary and proportionate reason for using it. Where audio is used, the school must assess the privacy impact, provide clear additional notice, restrict access and periodically review whether it remains justified.

1.5 The CCTV system is owned by the school, and its deployment is determined by the school's leadership team. The system is maintained and serviced by SET Digital IT Services. The school remains responsible for deciding why and how personal data is processed and for ensuring that any service provider's access is appropriately authorised and controlled.

1.6 The CCTV is monitored centrally from the Site office and the Assistant Headteachers office (located in The Vine)

1.7 The introduction of, or changes to, CCTV monitoring will be subject to consultation with staff and the school community.

1.8 CCTV images and any recorded sound that identify individuals are personal data. The school will process them in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (as amended), and other applicable law. This policy should be read alongside the school's Data Protection Policy, Data Security Policy, retention arrangements and Privacy Notice.

1.9 All authorised operators and employees with access to images or sound must understand and follow the school's procedures. Relevant staff must receive appropriate training on their responsibilities, confidentiality, secure handling, access requests and disclosure. Access must be limited to what is necessary for each person's role.

2. Statement of Intent

2.1 The school will follow applicable data protection law and the Information Commissioner's Office (ICO) guidance on video surveillance and CCTV. The guidance is available at:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdfhttps://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/cctv-and-video-surveillance/guidance-on-video-surveillance-including-cctv/

Clear, prominent and readable CCTV signs must be displayed before people enter monitored areas and, where appropriate, within those areas. Signs must explain that CCTV is in operation, state the purpose, identify the organisation operating the system and provide contact details or direct people to further privacy information. Because the system has sound-recording capability, any use of audio must be separately and clearly explained.

2.2 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.

Siting the Cameras

2.3 Cameras must be positioned to capture only what is necessary for the school's documented purposes. The school will consider privacy expectations, particularly because pupils may be vulnerable, and will restrict or mask views that are not needed. The school must identify and document a lawful basis for processing and assess privacy risks before introducing or materially changing surveillance.

2.4 The school will make every effort to position cameras so that their coverage is restricted to the school premises, which may include outdoor areas.

2.5 CCTV will not be used in classrooms.

2.6 Members of staff should have access to details of where CCTV cameras are situated.

2.7 Before introducing CCTV or making a material change to its use, the school will document the purpose, necessity, proportionality and lawful basis. A Data Protection Impact Assessment (DPIA) must be completed where the processing is likely to result in a high risk to individuals; the school should review the existing assessment when risks or system functions change.

2.8 The use of CCTV must be explained in the school's relevant Privacy Notices, including its purposes, lawful basis, retention period, recipients, individual rights and how to contact the school or its Data Protection Officer. Notices must be kept accurate when the system or its use changes.

3. Covert Monitoring

3.1 The school may, in exceptional circumstances, set up covert monitoring. For example:

i) Where there is good cause to suspect that an illegal or unauthorised action(s), is taking place, or where there are grounds to suspect serious misconduct;
ii) Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

3.2 In these circumstances authorisation must be obtained from a member of the senior management team.

3.3 Covert monitoring must cease following completion of an investigation.

3.4 Cameras sited for the purpose of covert monitoring will not be used in areas which are reasonably expected to be private, for example toilets.

4. Storage and Retention of CCTV images

4.1 CCTV footage will be kept only for as long as necessary for the documented purpose. The school currently retains routine footage for approximately 30 days before automatic deletion; this period must be reviewed periodically and justified against the school's needs. Relevant footage may be retained for longer where necessary for a specific incident, complaint, safeguarding matter, legal claim or law-enforcement investigation, with the reason documented and access restricted. Footage must be securely deleted when no longer required.

4.2 All retained footage and sound must be stored securely, with access controls and appropriate safeguards against unauthorised access, alteration, disclosure or loss. The school must be able to retrieve relevant footage promptly, preserve its integrity and securely delete it in accordance with the retention arrangements.

5. Access to CCTV images

5.1 Access to live or recorded images and sound is restricted to authorised people who need it for a defined school purpose. Access and disclosures should be recorded where appropriate, and footage must not be viewed, copied or shared for personal reasons or made more widely available.

6. Subject Access Requests (SAR)

6.1 Individuals may request access to their personal data contained in CCTV footage under the right of access in the UK GDPR. Requests may be made verbally or in writing and should be passed promptly to the Headteacher or the school's designated data-protection contact.

6.2 Requests should be directed to the Headteacher or the school's designated data-protection contact. The school may ask for proportionate information, such as the date, approximate time, location and a description of the requester, to help locate the footage. Requests must be handled promptly, and relevant footage should be protected from routine deletion while the request is being considered.

6.3 The school will respond without undue delay and normally within one month of receiving a valid request. Where the request is complex or multiple requests have been made, the period may be extended by up to a further two months; the requester must be informed of the extension and reasons within the first month.

6.4 The school should ensure that relevant footage can be located and exported in a commonly usable format. If a request concerns footage that may be overwritten during the response period, the school should preserve the relevant extract while the request is handled.

6.5 The school will consider the rights and freedoms of other people shown or heard in the footage. Where necessary, it may redact or obscure third parties' personal data. Access may be restricted or refused only where a relevant legal exemption applies; the school will explain its decision as appropriate.

7. Right to erasure

Under Article 17 of the UK GDPR, individuals may request erasure of their personal data in certain circumstances. This right is not absolute and does not automatically require CCTV footage to be deleted. The school will assess each request against the applicable law and any need to retain footage for legal obligations or the establishment, exercise or defence of legal claims.

When does the right to erasure apply?

Individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- the individual withdraws consent and there is no other lawful basis for continuing the processing;
- the individual objects to processing based on legitimate interests and there are no overriding legitimate grounds to continue;
- you are processing the personal data for direct marketing purposes and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- erasure is required to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child.

When does the right to erasure not apply?

The right to erasure does not apply if processing is necessary for one of the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

In the case of such a request the school would have to consider the request and respond to confirm whether or not they are able to comply with it. Within the school CCTV system all images are retained for approximately 30 days before being deleted automatically.

8. Access to and Disclosure of Images to Third Parties

8.1 Footage will only be disclosed where lawful, necessary and authorised, for example to the police, safeguarding authorities, insurers, legal advisers or contracted service providers where appropriate. The school will check the purpose and authority for disclosure, share only the relevant material, use secure transfer methods and keep a record of significant disclosures. A service provider's access must be governed by appropriate contractual and security arrangements.

8.2 Requests should be made in writing to the Headteacher.

8.3 The data may be used within the school's discipline and grievance procedures as required and will be subject to the usual confidentiality requirements of those procedures.

9. Complaints

9.1 Complaints and enquiries about the operation of CCTV should be directed to the Headteacher or the school's designated data-protection contact. Individuals may also raise concerns with the Information Commissioner's Office.

9.2 Where a complaint concerns the security, access, disclosure or retention of personal data, the school's Data Protection Officer or designated data-protection contact must be informed.

Further Information

Further information on CCTV and its use is available from the following:

- ICO guidance on video surveillance and CCTV (current online guidance)
- www.ico.gov.ukhttps://ico.org.uk/
- Regulation of Investigatory Powers Act 2000, where applicable (including any relevant amendments and current guidance)
- UK General Data Protection Regulation and Data Protection Act 2018 (as amended)
- Data Protection Policy
- Data Security Policy
- School's Privacy notice

Main School Building

One camera is in the Hydro Pool Entrance, and a second camera is located in the Main Reception

Hydro Pool Entrance



Main Reception



One camera is located in the Hydro Pool area and is used for safety and security purposes.

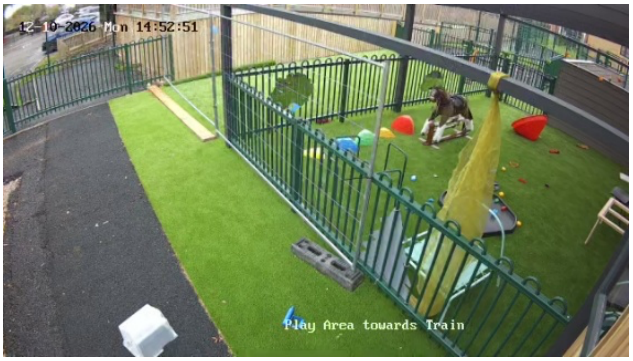
Hydro Pool



The Vine



Main Entrance



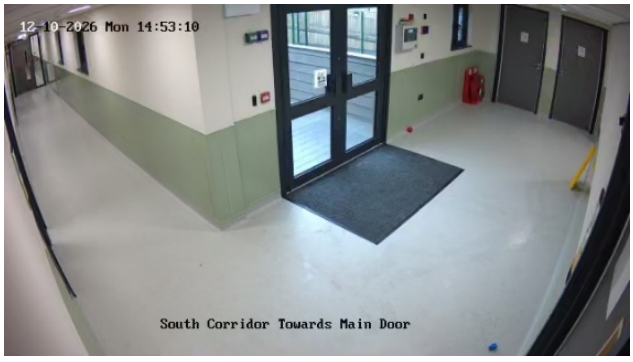
Play Area Towards Train



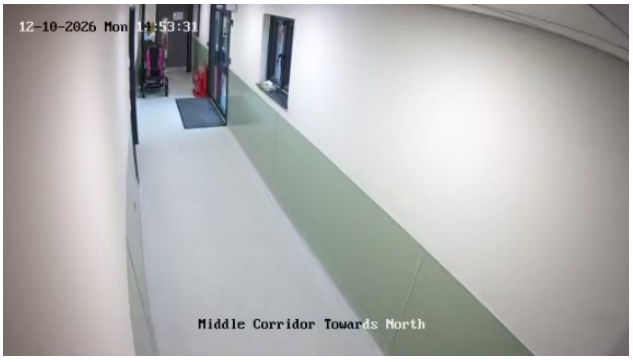
Towards Plant Room / Sensory



Side Towards School



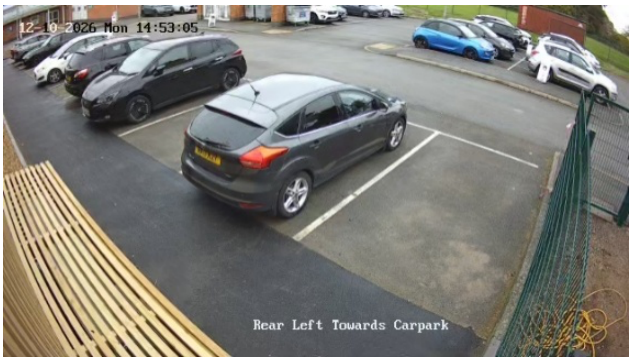
South Corridor Towards Main Door



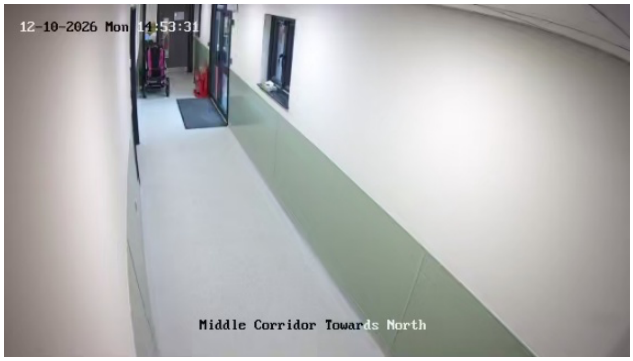
Middle Corridor Towards North



North Corridor Towards Entrance Doors



Rear Left Towards Car Park



Middle Corridor Towards North



Middle Corridor Towards North



Towards Air Lock Entrance Gates