CCTV Policy

September 2025

Weaver Trust

Inspire - Believe - Achieve

At Weaver Trust, we work to ensure that all in our community believe, belong, and thrive. This policy is informed by our Trust's vision of inspiring all to believe in their own ability to achieve their full potential, both academically and socially. By living by our values of being innovative, responsible and caring, we create powerful learning communities - positively impacting all.

1. Policy Statement

1.1. This policy outlines the school's approach to the operation, management, and usage of surveillance and closed-circuit television (CCTV) systems on school property.

2. Definitions

Term	Definition
Trust	Is Weaver Trust Limited, Suite 2, Oak Tree Barn, Hatton Lane, Warrington, WA4 4BX and its subsidiary organisations, and clubs, collectively referred to as the 'Trust'
Department for Education (DfE)	Is the government department which deals with education
Local Authority (LA)	is Cheshire West and Chester Council, The Portal, Wellington Road, Ellesmere Port, CH65 0BA or Halton Borough Council, Municipal Building, Kingsway, Widnes, Cheshire, WA8 7QF
Chief Executive Officer (CEO)	Is Annette Williams
Chief Operating Officer (COO)	Is Annette Williams
Trust Governance and Communications Manager	Is Phil Atkinson
Data Protection Coordinator	Is Phil Atkinson
System Manager	Is Dean Stening
Trust Data Protection Officer (DPO)	Is Tru-Digital Protection T/A Tru-Digital Services Ltd, 5 Brayford Square, London, E1 0SG dpo@trudigital.co.uk
Surveillance	Is the act of watching a person or a place

CCTV	Is Closed Circuit Television; video cameras used for surveillance
Covert Surveillance	Is the operation of cameras in a place where people have not been made aware that they are under surveillance

3. Introduction

3.1 Statement of Intent

3.1.1 The purpose of the CCTV system is to:

- Make members of the school community feel safe.
- Protect members of the school community from harm to themselves or to their property.
- Deter criminality in the school.
- Protect school assets and buildings.
- Help the police prevent and identify crimes.
- Determine the cause of accidents.
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defence of any litigation proceedings

3.1.2 The CCTV system will not be used to:

- Encroach on an individual's right to privacy.
- Monitor people in spaces where they have a heightened expectation of privacy (including toilet areas and changing rooms).
- Follow particular individuals, unless there is an ongoing emergency incident occurring.
- Pursue any other purposes other than the ones stated above.

3.1.3 The list of uses of CCTV is not exhaustive, and other purposes may be or become relevant.

3.1.4 The CCTV system is registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and the UK GDPR.

3.1.5 Footage or any information gleaned through the CCTV system will never be used for commercial purposes.

3.1.6 In the unlikely event that the police request that CCTV footage be released to the media, the request will only be complied with when written authority has been provided by the police, and only to assist in the investigation of a specific crime.

3.1.7 The footage produced by the system should be of sufficient quality to assist the police or the court in identifying suspects.

3.1.8 This policy must be approved by the governing body and signed by the Headteacher and the Chair of Governors.

4. Relevant Legislation and Guidance

4.1 This policy refers to and complies with the following legislation and guidance:

- UK General Data Protection Regulation
- Data Protection Act 2018
- Human Rights Act 1998
- European Convention on Human Rights
- The Regulation of Investigatory Powers Act 2000
- The Protection of Freedoms Act 2012
- The Education (Pupil Information) (England) Regulations 2005 (as amended in 2016)
- The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004
- The School Standards and Framework Act 1998
- The Children Act 1989
- The Children Act 2004
- The Equality Act 2010
- Surveillance Camera Code of Practice (2021)

5. Covert Surveillance

5.1 Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If covert surveillance is needed (such as following police advice for the prevention or detection of crime or where there is a risk to public safety), a data protection impact assessment will be completed to comply with data protection law.

6. Location of the Cameras

6.1 Cameras are located in places that require monitoring to achieve the aims of the CCTV system (stated in section 3.1).

6.2 Cameras are sited in locations such as:

- Office Reception

- Corridors

6.3 Cameras are not and will not be aimed at school grounds, public spaces or people's private property.

6.4 Cameras are positioned to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

7. Roles and Responsibilities

7.1 The Governing Board

7.1.1 The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 4) is complied with.

7.2 The Headteacher

7.2.1 The headteacher will:

- Take responsibility for all day-to-day leadership and management of the CCTV system.
- Liaise with the data protection officer (DPO) to ensure that the use of the CCTV system is in accordance with the stated aims and that its use is needed and justified.
- Ensure that all staff follow the guidance set out in this policy.
- Review the CCTV policy to check that the school is compliant with legislation.
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection.
- Sign off on any expansion or upgrading to the CCTV system after having taken advice from the DPO and having taken into account the result of a data protection impact assessment.
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties.

7.3 The Business Manager or Data Protection Coordinator

7.3.1 The DPO will:

- Train persons with authorisation to access the CCTV system and footage in the use of the system, and in data protection
- Deal with subject access requests in line with the UK GDPR and Data Protection Act 2018
- Conduct data protection impact assessments
- Ensure data is handled in accordance with data protection legislation
- Ensure footage is obtained in a legal, fair and transparent manner
- Ensure footage is destroyed when it falls out of the retention period
- Keep accurate records of all data processing activities and make the records public on request
- Inform subjects of how footage of them will be used by the school, what their rights are, and how the school will endeavour to protect their personal information

- Ensure that the CCTV systems are working correctly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system does not infringe on any individual's reasonable right to privacy in public spaces
- Carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period
- Receive and consider requests for third-party access to CCTV footage

7.4 The DPO

7.4.1 The DPO will:

- Train all staff to recognise a subject access request
- Support with subject access requests in line with the UK GDPR and Data Protection Act 2018
- Monitor compliance with UK data protection law
- Advise on and assist the school with carrying out data protection impact assessments
- Act as a point of contact for communications from the Information Commissioner's Office (ICO)
- Support data protection impact assessments
- Support requests for third-party access to CCTV footage

7.5 The System Manager

7.5.1 The System Manager will:

- Take care of the day-to-day maintenance and operation of the CCTV system.
- Conduct data protection impact assessments.
- Oversee the security of the CCTV system and footage.
- Ensure that the CCTV systems are working correctly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified.
- Check the system for faults and security flaws on a regular basis.
- Ensure the data and timestamps are accurate on a termly basis.

8. Operation of the CCTV System

8.1 The CCTV system will be operational 24 hours a day, 365 days a year.

8.2 The system is registered with the Information Commissioner's Office.

8.3 The system will not record audio.

8.4 Recordings will have a date and time stamps. The system manager will check these periodically, and when the clocks change.

9. Storage of CCTV Footage

9.1 Footage will be retained for 30 days. The files will be overwritten automatically at the end of the retention period.

9.2 Occasionally, footage may be retained for longer than 30 days, for example, when a law enforcement body is investigating a crime, to allow them to view the images as part of an active investigation.

9.3 Recordings will be downloaded and encrypted, ensuring the data remains secure and intact. This will allow for the use of the recordings as evidence if required.

9.4 The Headteacher will conduct termly checks to determine whether the footage is being stored accurately and deleted after the retention period.

10. Access to CCTV Footage

10.1 Access will only be given to authorised persons to pursue the aims stated in section 1.1 or if there is a lawful reason to access the footage.

10.2 Any individuals who access the footage must record their name, the date and time of access, and the reason for access in the access log.

10.3 Any visual display monitors will be positioned so that only authorised personnel can see the footage.

10.4 Staff Access

10.4.1 The following members of staff have authorisation to access the CCTV footage:

- The Headteacher.
- The Deputy Head.
- The Data Protection Coordinator.
- The DPO.
- The System Manager.
- Anyone with express permission from the headteacher.

10.4.2 CCTV footage will only be accessed from authorised personnel's work devices or the visual display monitors.

10.4.3 All staff members with access will undergo training to ensure the proper handling of the system and footage.

10.4.4 Any member of staff who misuses the surveillance system may be committing a criminal offence and will face disciplinary action.

10.5 Subject Access Requests (SARs)

10.5.1 According to GDPR and the DPA, individuals can request a copy of any CCTV footage of themselves and only themselves.

10.5.2 Upon receiving the request, the school will immediately issue a receipt and respond within 30 school days during term time. Due to difficulties accessing appropriate staff members, the school reserves the right to extend that deadline during holidays.

10.5.3 All staff have received training to recognise SARs. When a SAR is received, staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information, such as the date, time, and location of the footage taken, to aid school staff in locating the footage.

10.5.4 Occasionally, the school reserves the right to refuse a SAR if, for example, releasing the footage to the subject would prejudice an ongoing investigation or the interests of a person(s).

10.5.5 Images that may identify other individuals must be obscured to prevent unwarranted identification. The school will provide still images with their identities concealed by blurring out their faces. If this is not possible, the school will seek their consent before releasing the footage. If consent is not forthcoming, we will refuse the release of the footage.

10.5.6 The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with a repetitive, unfounded, or excessive SAR.

10.5.7 Footage disclosed in a SAR will be disclosed securely to ensure that only the intended recipient can access it.

10.5.8 Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

10.5.9 Individuals wishing to make a SAR can find more information about their rights, the process of submitting a request, and what to do if they are dissatisfied with the response on the ICO website.

10.6 Third-Party Access

10.6.1 CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 3.1 (e.g. assisting the police in investigating a crime).

10.6.2 Footage will only be shared with authorised personnel such as law enforcement agencies or other service providers who reasonably need access to the footage (e.g. investigators).

10.6.3 All access requests should be set out in writing and sent to the Headteacher and the DPO.

10.6.4 The school will comply with any court orders that grant access to the CCTV footage. The school will provide the courts with the necessary footage, but not grant them unrestricted access. The DPO will carefully consider how much footage to disclose and seek legal advice if necessary.

10.6.5 The DPO will ensure that any disclosures are made in compliance with GDPR.

10.6.6 The DPO will record all disclosures.

11. Data Protection Impact Assessment (DPIA)

11.1 The school follows the principle of privacy by design. Privacy is considered at every stage of the CCTV system's deployment, including replacement, development, and upgrading.

11.2 The system is used only to fulfil its aims (stated in section 3.1).

11.3 When the CCTV system is replaced, developed, or upgraded, a DPIA will be carried out to ensure that its aim remains justifiable, necessary, and proportionate.

11.4 The DPO will provide guidance on how to conduct the DPIA, which will be conducted by the System Manager.

11.5 Those whose privacy is most likely to be affected, including the school community and neighbouring residents, will be consulted during the DPIA, and any appropriate safeguards will be implemented.

11.6 A new DPIA will be performed annually or whenever cameras are moved or new cameras are installed.

11.7 If any security risks are identified during the DPIA, the school will address them immediately.

12. Security

12.1 The System Manager or Data Protection Coordinator will be responsible for overseeing the security of the CCTV system, footage and the Electronic Platform.

12.2 The system will be checked for faults once a term.

12.3 Any faults in the system will be reported as soon as they are detected and repaired as quickly as possible, according to the proper procedure.

12.4 Footage will be stored securely and encrypted wherever possible.

12.5 The CCTV footage will be password-protected, and any camera operation equipment will be securely locked away when not used.

12.6 Any software updates (mainly security updates) published by the equipment manufacturer that require application will be applied as soon as possible.

Approved by: _____ _____

Chair of Trust **CEO**

Date: _____ _____