



HEARTWOOD

LEARNING TRUST

CCTV POLICY

THIS POLICY APPLIES TO THE TRUST BOARD, THE CENTRAL SERVICES TEAM
AND ALL TRUST SCHOOLS/ACADEMIES

Document Management	
Updated Policy Approved	September 2024
Next Review Date	September 2025 <i>(Extended until 31st March 2026)</i>
Version	3.0
Approved By	Chief Operating Officer

Contents

Policy Updates	2
Statement of Intent	3
1. Introduction	4
2. Definition	4
3. Legal Framework	4
4. Roles and Responsibilities	5
5. Objectives	7
6. Purpose and Justification	7
7. Operation of the System/Security	7
8. Data Protection	8
9. Monitoring Procedures	9
10. Media Procedures	9
11. Breaches of the Code of Practise (including Breaches of Security)	10
12. Assessment of the scheme and code of practice	10
13. Complaints	10
14. Code of Practice	10
15. Access	11
16. Monitoring and Review	12
Appendix 1 - Localised Procedures	13

Policy Updates

Date	Page	Policy Updates
June 2022	4	Legal Framework section added
June 2022	6	Operations of the System/Security section added
June 2022	7	Data Protection – ‘Privacy by Design’ from previous copy removed and renamed with updated information
June 2022	9	Code of Practice section added
June 2022	10	Monitoring and Review section added
October 2023	Whole Policy	Updated inline with the new Scheme of Delegation
September 2024	4	2 - Terms added to ‘definitions’
September 2024	5	3 - Minor updates to legal framework and addition of linked Trust policies
September 2024	6	4.5 - New responsibilities assigned to the data controller
September 2024	7	7.1, 7.4, 7.6, 7.10, 7.11 - Points added/amended for clarity
September 2024	10	11.1 - Amended to reflect localised procedures
September 2024	11	14.9-14.13 - Points added regarding biometric information security
September 2024	11	15.10-15.11 - Points added regarding ‘Right to Erasure’
September 2024	12	15.7-15.8 - Points added to clarify circumstances of releasing CCTV footage/images
September 2024	13	Appendix 1 - Added to include localised procedures in one central area, in line with other Trust policies

Statement of Intent

Heartwood Learning Trust takes responsibility towards the safety of staff, visitors and pupils very seriously. To that end, the Trust uses surveillance cameras to monitor any instances of aggression or physical damage to the academies/schools within the Trust.

The purpose of this policy is to regulate the management, operation and use of the surveillance and closed-circuit television (CCTV) system in the academies/schools within Heartwood Learning Trust where applicable, hereafter referred to as 'the school/academy'.

The CCTV Scheme will be registered with the Information Commissioner under the terms of the UK General Data Protection Regulation and will seek to comply with the requirements of both GDPR and the Commissioner's Code of Practice.

The Trust will treat the systems and all information, documents and recordings obtained and used as data which is protected by GDPR.

Each school/academy will not focus static cameras on private homes, gardens and other areas of private property.

Unless an immediate response to events is required, each school/academy will not direct cameras at an individual, their property or a specific group of individuals, without authorisation being obtained using the school/academy's forms for Directed Surveillance to take place, 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. Media forms will only be released for use in the investigation of a specific crime and with the written authority of the Police. CCTV footage will never be released to the media for purposes of entertainment.

The planning and design has 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.

Warning signs, as required by the Code of Practice of the Information Commissioner, have been placed at all access routes to areas covered by the school/academy CCTV.

The CCTV system will be registered with the ICO in line with data protection legislation.

1. Introduction

- 1.1. The system comprises of:
 - Cameras - fixed
 - Cameras - dome
- 1.2. The Code of Practice will be subject to review periodically, but at least biennially, to include consultation as appropriate with interested parties.
- 1.3. The CCTV system is owned by the school/academy.

2. Definition

- 2.1. The CCTV is the '**Closed Circuit Television System**' which is used within the school/academy buildings and grounds only. The system is monitored locally within each school/academy and is used for 'Application' purposes only.
- 2.2. **Surveillance** - monitoring the movements and behaviour of individuals; this can include video, audio or live footage e.g. real-time recordings and live streams. For the purpose of this policy only video and audio footage will be applicable.
- 2.3. **Overt surveillance** - this is surveillance which is clearly visible and signposted around the school/academy. Overt surveillance does not fall under the Regulation of Investigatory Powers Act 2000.
- 2.4. **Covert surveillance** - this is surveillance that subjects are intentionally not informed about and recordings are concealed. Covert surveillance is not permitted under any circumstances.
- 2.5. **Biometric data** - data which is related to the physiological characteristics of a person, which confirm the unique identification of that person such as fingerprint recognition, facial recognition (FRT), or iris recognition.
- 2.6. **Automated biometric recognition system** - a system which uses technology to measure an individual's physical or behavioural characteristics by using equipment that operates 'automatically'.
- 2.7. **Facial recognition** - the process by which a person can be identified or otherwise recognised from a digital facial image. Cameras are used to capture these images and facial recognition technology software produces a biometric template.

3. Legal Framework

- 3.1. This policy has due regard to legislation, including but not limited to the following:
 - The UK General Data Protection Regulation (UK GDPR)
 - The Data Protection Act 2018
 - Freedom of Information Act 2000

- Protection of Freedoms Act 2012
- School Standards and Framework Act 1998
- Children Act 1989 and 2004
- Equality Act 2010
- Surveillance Camera Code of Practice 2013
- Regulation of Investigatory Powers Act 2000
- The Education (Pupil Information)(England) Regulations 2005 (as amended in 2016)

3.2. This policy has been created with regard to the following statutory and non-statutory guidance:

- DfE (2022) 'Protection of biometric data of children in schools and colleges
- 'The Surveillance Camera Code of Practice' - Home Office (2021)
- 'Guide to the UK General Data Protection Regulation (UK GDPR) ICO 2021
- 'In the picture: A data protection code of practice for surveillance cameras and personal information' ICO (2017)
- ICO (2022) 'Video Surveillance'

3.3. This policy operates in conjunction with the following Trust policies:

- Photography and Videos in Schools Policy
- E-Safety and Acceptable Use Policy - Pupils
- E-Safety and Acceptable Use Policy - Staff and Authorised Users
- Freedom of Information Policy
- Data Protection (UK GDPR) Policy

4. Roles and Responsibilities

4.1. Trust Board

The Trust Board is ultimately responsible for the systems and ensuring compliance with each school/academy.

4.2. Data Protection Officer (DPO)

The role of the Data Protection Officer (DPO) includes:

- Dealing with Freedom of Information requests and Subject Access Requests (SARs) in line with legislation, including the Freedom of Information Act 2000.
- Ensuring that all data controllers at the school/academy handle and process surveillance and CCTV footage in accordance with data protection legislation.
- Ensuring that surveillance and CCTV footage is obtained in line with legal requirements.
- Ensuring that surveillance and CCTV footage is destroyed in line with legal requirements when it falls outside of its retention period.
- Keeping comprehensive and accurate records of all data processing activities, including surveillance and CCTV footage, detailing the purpose of the activity and making these records public upon request.

- Informing data subjects of how their data captured in surveillance and CCTV footage will be used by the school/academy, their rights for the data to be destroyed and the measures implanted by the school/academy to protect individuals' personal information.
- Abiding by confidentiality requirements in relation to the duties undertaken while in the role.
- Monitoring the performance of the school/academy's Data Protection Impact Assessment (DPIA) and providing advice where requested.
- Presenting reports regarding data processing at the school/academy to relevant personnel.

4.3. **Headteacher/Principal**

The Headteacher/Principal is responsible for:

- Delegating day-to-day matters relating to data protection to a local nominated GDPR Representative.
- Ensuring that the local nominated **GDPR Representative** undertakes appropriate training
- That there is a school based provision for reporting data breaches at all times within the school/academy including school holidays/closures.
- Ensuring the school/academy reports data breaches within the defined timescales detailed within the Trust's Data Breach Policy and Procedures.
- Conferring with the DPO with regard to the lawful processing of the surveillance and CCTV footage.
- Reviewing the CCTV Policy to ensure it is compliant with current legislation.
- Monitoring legislation to ensure the school/academy is using surveillance fairly and lawfully.
- Communicating any changes to legislation with all members of staff.

4.4. **Nominated GDPR Representative(s)**

The designated person(s) deals with the day-to-day matters relating to data protection at the school/academy and thus, for the benefit of this policy, will act as the data controller.

4.5. **Data Controller**

The role of the Data Controller includes:

- Processing surveillance and CCTV footage legally and fairly.
- Collecting surveillance and CCTV footage for legitimate reasons and ensuring that it is used accordingly.
- Collecting surveillance and CCTV footage that is relevant, adequate and not excessive in relation to the reason for its collection.
- Ensuring that any surveillance and CCTV footage identifying an individual is not kept for longer than is necessary.
- Protecting footage containing personal data against accidental, unlawful destruction, alteration and disclosure - especially when processing over networks.
- Ensuring that the processing of any biometric data, including any processing carried out by a third party on their behalf complies with the Data Protection Act 2018, UK GDPR and Protection of Freedoms Act 2012.
- Identifying the additional risks associated with using automated biometric technology by conducting a DPIA ensuring decisions are documented.

- Ensuring that the processing of biometric data is done so in line with the Trust's Protection of Biometric Data Policy.

5. Objectives

- 5.1. To protect the school/academy building and their assets. The systems function is to:
- Maintain a safe environment
 - Ensure the welfare of pupils, staff and visitors
 - Deter criminal acts against persons and property
 - Assist the Police in identifying persons who have committed an offence

6. Purpose and Justification

- 6.1. The school/academy will only use surveillance cameras for the safety and security of the school/academy and its staff, pupils and visitors.
- 6.2. Surveillance will be used as a deterrent for violent behaviour and damage to the school/academy.
- 6.3. The school/academy will only conduct surveillance as a deterrent and under no circumstances will the surveillance and the CCTV cameras be present in classrooms or any changing facility.
- 6.4. If the surveillance and CCTV systems fulfil their purpose and are no longer required the school/academy will deactivate them.

7. Operation of the System/Security

- 7.1. The administration and management of the system, where appropriate, is delegated by the **Headteacher/Principal** to the site teams, in accordance with this policy. In the event that there is not a site team associated with the school/academy, the Headteacher/Principal will nominate an appropriate colleague to undertake this task.
- 7.2. The CCTV system will be operated 24 hours each day, every day of the year.
- 7.3. The **site team** will check and confirm the efficiency of the system on a monthly basis and that the equipment is properly recording and that cameras are functional.
- 7.4. In exceptional cases where large amounts of information need to be collected and retained, the school will seek advice from the central team, who may consider cloud storage. This will be secure and only accessible to authorised individuals.
- 7.5. The ability to produce copies of information will be limited to the appropriate staff.

- 7.6. The system will be restricted to limited operators (such as the Senior Leadership Team and Site Team) and will be password protected. Please refer to [Appendix 1](#) for details of the operators responsible for the school/academy's CCTV operations.
- 7.7. Surveillance and CCTV systems will not be intrusive.
- 7.8. Any unnecessary footage captured will be securely deleted from the system.
- 7.9. Any cameras that present faults will be repaired as soon as possible to avoid any risk of a data breach.
- 7.10. The system may generate a certain amount of interest. It is vital that operations are managed, by authorised individuals with the minimum of disruption.
- 7.11. Please refer to [Appendix 1](#) for details of locations where visual display/control monitors are located.
- 7.12. Staff will be trained in the use of the CCTV system and sanctions will be put in place for those who misuse the security system information.

8. Data Protection

- 8.1. Data collected from surveillance and CCTV will be:
 - Processed lawfully, as determined by a DPIA, or from advice from the DPO.
 - Processed fairly, in a manner that people would reasonably expect, and taking into account advancements in technology that may not be anticipated by some people.
 - Processed in a transparent manner, meaning that people are informed when their data is being captured.
 - Collected for specified and legitimate purposes – data will not be processed further in a manner that is incompatible with the following purposes:
 - Further processing for archiving data in the public interest
 - Scientific or historical research
 - Statistical purposes
 - Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
 - Accurate, and where necessary, kept up-to-date, every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay.
 - Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.
- 8.2. The use of surveillance cameras, CCTV and biometric systems, will be critically analysed using a DPIA, in consultation with the DPO.

- 8.3. A DPIA will be carried out prior to the installation of any surveillance, CCTV or biometric system. A DPIA will:
- Describe the nature, scope, context, and purposes of the processing
 - Assess necessity, proportionality and compliance measures
 - Identify and assess risks to individuals
 - Identify any additional measures to mitigate those risks
- 8.4. If the DPIA reveals any potential security or other data protection issues, the Trust will ensure they have provisions in place to overcome these issues.
- 8.5. Where the Trust identifies a high risk to an individual's interests, and it cannot be overcome, the Trust will consult with the ICO before they use CCTV and the Trust will act on the ICO's advice.

9. Monitoring Procedures

- 9.1. Camera surveillance may be maintained at all times. Approved personnel may have remote access to the CCTV system via their school/academy hardware for security purposes.

10. Media Procedures

- 10.1. In order to maintain and preserve the integrity of the media used to record events from the hard drive and the facility to use them in any future proceedings, the following procedures for their use and retention must be strictly adhered to:
- a. Before using, each media form must be cleaned of any previous recording.
 - b. The controller shall register the date and time of media form insert, including media reference.
 - c. If copies of the media form are required for the Police, these must be referenced and marked 'copy'.
- 10.2. Media forms may be viewed by the Police for the prevention and detection of crime. A register will be maintained of the release of media form to the Police or other authorised applicants. The register will be available for review by the Trust Operations Manager, or a designated colleague, at all times.
- 10.3. Viewing of Media by the Police must be recorded in writing and in the register. Requests by the Police can only be actioned under Section 19 of GDPR 2018.
- 10.4. Should a media form be required as evidence, a copy may be released to the Police under the procedures of the Code of Practice for Surveillance cameras and personal Information 2017. Media will only be released to the Police on the clear understanding that the media form remains the property of the school/academy and both the media form and information contained on it are to be treated in accordance with this Code. The school/academy also retains the right to refuse permission for the Police to pass to any other person the media form or any part of the information contained thereon.

- 10.5. The Police may require the school/academy to retain the stored media for possible use as evidence in the future. Such media will be correctly indexed and securely stored until they are needed by the Police.
- 10.6. Applications received from outside bodies (e.g. solicitors) to view or release media will be referred to the Headteacher/Principal.

11. Breaches of the Code of Practise (including Breaches of Security)

- 11.1. Any breach of the Code of Practice by school/academy staff will be investigated by the appropriate person(s) in order for them to take the appropriate disciplinary action. Any breach of the Code will be reported to the Board of Trustees. Full details of the person(s) responsible for initial investigations can be found within [Appendix 1](#).
- 11.2. Any serious breach of the Code of Practice will be immediately investigated, and an independent investigation carried out to make recommendations on how to remedy the breach.

12. Assessment of the scheme and code of practice

- 12.1. Performance monitoring, including random operating checks, may be carried out by the **site team**, or in the event that a site team is not on site, a nominated individual.

13. Complaints

- 13.1. Complaints about the academy's/school's CCTV system should be addressed to the **Headteacher/Principal**. Complaints will be investigated in accordance with this Code and the Trust's Complaints Policy and Procedure.

14. Code of Practice

- 14.1. The school/academy understands that recording images of identifiable individuals constitutes processing personal information, so it is done in line with data protection principles.
- 14.2. The school/academy notifies all pupils, staff and visitors of the purpose for collecting surveillance data via notice boards, letters and emails
- 14.3. CCTV cameras are only placed where they do not intrude on anyone's privacy and are necessary to fulfil their purpose.
- 14.4. All surveillance footage will be kept for approximately **one calendar month** (or 30 days) for security purposes; the Headteacher/Principal is responsible for keeping the records secure and authorising access.
- 14.5. The school/academy has a surveillance system for the purpose of the prevention and detection of crime and the promotion of health, safety and welfare of staff, pupils and visitors.

- 14.6. The surveillance and CCTV system is owned by the school/academy and images from the system are strictly controlled and monitored by authorised personnel only.
- 14.7. The school/academy will ensure that the surveillance and CCTV system is used to create a safer environment for staff, pupils and visitors to the school/academy, and to ensure that its operation is consistent with the obligations outlined in data protection legislation. The policy is available from the school/academy website.
- 14.8. The surveillance and CCTV system will:
- Be designed to take into account its effect on individuals and their privacy and personal data.
 - Be transparent and include a contact point which enables people to request information and submit complaints via the DPO.
 - Only keep images and information for as long as required.
 - Restrict access to retained images and information with clear rules on who can gain access.
 - Only be used for the purpose for which it is intended, including supporting public safety, the protection of pupils, staff and volunteers, and law enforcement.
 - Be accurate and well maintained to ensure information is up-to-date.
- 14.9. To comply with the requirements of the Protection of Freedoms Act 2012, the school/academy will notify all parents/carers of its intention to process pupils' biometric data, and emphasise that parents/carers may object at any time to the processing of the information.
- 14.10. The school/academy will ensure that pupils' biometric data is not taken or used as part of a biometric recognition system if pupils under the age of 18 object or refuse to participate in activities that involve the processing of their biometric data. The school/academy is aware that a pupil's objection or refusal overrides any parental consent to the processing of data.
- 14.11. The school/academy will ensure that information is included in its privacy notices that explains how biometric data is to be processed and stored, including the rights available to individuals in respect of the processing.
- 14.12. Reasonable alternative arrangements will be provided for pupils who do not use automated biometric recognition systems either because their parents have refused consent or due to the pupil's own refusal to participate in the collection of their biometric data.
- 14.13. The alternative arrangements will ensure that pupils do not suffer any disadvantage or difficulty in accessing services and premises. Likewise, such arrangements will not place any additional burden on parents whose children are not participating in such a system.

15. Access

- 15.1. The UK GDPR provides Data Subjects (individuals to whom "personal data" relates) with a right to obtain confirmation that their personal data is being processed and to access personal data held about themselves, including data obtained by CCTV.

- 15.2. Individuals have the right to have their personal data erased if:
- The data is no longer necessary for the original purpose it was collected for.
 - The data processor relies on legitimate interests as a basis for processing, the data subject objects to the processing of their data, and there is no overriding legitimate interest to continue the processing.
 - The data has been processed unlawfully.
 - There is a specific legal obligation.
- 15.3. There are certain exceptions where the right to erasure cannot be exercised, these include, but are not limited to:
- Where the processing is needed for the performance of a task in the public interest or an official authority.
 - Certain research activities.
 - Compliance with a specific legal requirement.
- 15.4. All media captured by CCTV imaging belongs to, and remains the property of the school/academy.
- 15.5. The school/academy will verify the identity of any person(s) making a Subject Access Request (SAR) before any information is supplied. Please refer to the Trust's Subject Access Request Policy and Procedures for further details.
- 15.6. Requests by persons outside the school/academy for viewing or copying disks, or obtaining digital recordings, will be assessed by the Headteacher/Principal, who will consult the DPO, on a case-by-case basis with close regard to data protection and freedom of information legislation.
- 15.7. It is important that access to, and disclosure of, the images recorded by surveillance and CCTV footage is restricted and carefully controlled, not only to ensure the rights of individuals are preserved, but also to ensure the chain of evidence remains intact, should the images be required for evidential purposes.
- 15.8. Release of recorded images to third parties will be permitted only where the Police require these images to assist in a specific criminal enquiry, in such circumstances release of images is permitted by law.

16. Monitoring and Review

- 16.1. This policy will be monitored and reviewed on **an annual basis** by the Trust Operations Manager (TOM) and approved by the Chief Operating Officer (COO). The next scheduled review date can be found on the title page of this document.
- 16.2. The Headteacher/Principal will communicate changes to this policy to all members of staff.

CCTV Policy	
Localised School Based Procedures	
School Name:	
Headteacher/Principal:	
Implementation Date: <i>Inline with policy approval</i>	

Introduction

In conjunction with the Trust wide CCTV Policy, localised procedures have been established to ensure that systems and procedures reflect the school/academy setting.

The localised procedures for the school/academy setting focuses on the following key areas:-

- CCTV Operators
- Locations of CCTV Visual Display/Control Monitors
- Person(s) responsible for investigating breaches of the code of practice/security breaches

Should you have any concerns or questions relating to the localised procedures, in the first instance, please contact hello@school.hlt.academy

Please see below names of person(s) authorised to access CCTV login details on behalf of the school/academy.

Details of Authorised CCTV Operators	
Relates to item 7.6 within the Trust CCTV Policy	
Name	Role

Please see the below location(s) within the school/academy site that CCTV footage can be viewed/accessed.

Locations of CCTV Visual Display/Control Monitors	
Relates to item 7.11 within the Trust CCTV Policy	

Please see the below details of the person(s) responsible for investigating breaches of the code of practice and/or security breaches.

Details of Person(s) Responsible for Investigating Breaches	
Relates to item 11.1 within the Trust CCTV Policy	
Name	Role