GREAT HEIGHTS ACADEMY TRUST

Achieving excellence together

CCTV Policy

Approved by:	Trust Board		
Responsible department:	Core MAT Team		
Last review date:	July 2023	**Last reviewed by:**	DPO/COO
Last updated:	July 2023	**Last updated by:**	DPO/COO
Next review due :	July 2025		

1. Introduction

1.1 A Closed Circuit Television (CCTV) System is in place in a number of Trust academies. This system, known as the 'CCTV System', comprises a number of cameras installed at strategic locations. All of the cameras are fully operational and are recording.

1.2 For the purpose of this policy, the 'Owner' of the system is the Trust.

1.3 For the purposes of the Data Protection Act 2018 ('DPA'), the 'Data Controller' is the Trust.

1.4 This policy will be subject to review periodically, but at least biannually, to include consultation with interested parties.

1.5 Throughout this policy it is intended, as far as possible, to balance the objectives of the CCTV System with the need to safeguard the individual's rights. Every effort has been made throughout this policy to indicate that a formal structure has been put in place for the use and processing of the CCTV system and its recordings.

2. Purpose and Scope of this policy and the use of CCTV in the academy

2.1 The purpose of this policy is to set out how the CCTV system will be used in academies, who is responsible for monitoring the system and how the Trust will comply with its obligations under the DPA and General Data Protection Regulations (GDPR) 2018.

2.2.1 CCTV is used in academies to protect the buildings and its assets, to protect the health and safety of pupils, staff and visitors and to help detect, prevent and reduce incidence of criminal activity.

2.2.2 The lawful basis for using CCTV footage is to allow the academies to perform the public task of offering education and safeguarding of pupils whilst keeping the premises safe.

3. Relationship with other policies

3.1 This policy should be read in conjunction with the following policies:

3.1.1 Data Protection Policy.

3.1 2 Records Management and Retention Policy.

4. Roles and Responsibilities

4.1 The Principal in each Academy is the overall manager of the CCTV System and responsible for ensuring the objectives and principles set out in this policy are upheld.

4.2 Key Personnel have day-to-day responsibility for the monitoring, operation and evaluation of the CCTV System and the implementation of this policy. Academy Principals are responsible for maintaining full information as to the incidents dealt with in the management of the CCTV System.

5. Principles

5.1 Each CCTV System is registered with the Information Commissioner's Officer and the relevant signs are displayed around sites to notify people of the use of CCTV.

5.2 Each CCTV System is operated in accordance with the DPA and the Information Commissioner's Code of Practice at all times.

5.3 Each CCTV System is operated in accordance with all the requirements and the principles of the Human Right Act 1998.

5.4 Each CCTV System is operated fairly, within the law, and only for the purposes for which it was established and those identified within this policy.

5.5 The public interest in the operation of each system is recognised by ensuring the security and integrity of operational procedures.

6. Cameras and Area Coverage

6.1 The areas covered by CCTV, to which this policy refers, are the buildings and grounds of the academy.

6.2 None of the cameras forming part of the system are installed in a covert manner. Some cameras may be enclosed within 'All weather domes' for aesthetic or operational reasons.

6.3 Each academy will make every effort to position cameras so that their coverage is restricted to the academy premises, which also includes outdoor areas.

6.4 CCTV will not be used in classrooms with the exception of isolation units.

6.5 Covert Monitoring may be set up in exceptional circumstances. For example:

- 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;
- Where notifying the individuals about the monitoring would seriously prejudice the reason for making the recording.

In these circumstances authorisation must be obtained from the Principal. Covert monitoring must cease following completion of an investigation.

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

Unless required for evidential purposes or the investigation of crime or otherwise required by law, covertly recorded images will be retained for no longer than 30 days from the date of recording.

7. Monitoring Equipment

7.1 The CCTV System records the images from all cameras in real time.

7.2 Access to the cameras, operating controls, recording and reviewing equipment is strictly limited to authorised personnel only.

7.3 Any authorised person operating the cameras always acts with utmost integrity.

7.4 Any replay of pre-recorded data is only undertaken in restricted areas.

7.5 Unauthorised persons do not have access to any part of the CCTV System without the authorisation of the Principal..

7.6 All CCTV operators receive training relevant to their role. Further training is provided as necessary.

8. Privacy and Data Protection

8.1 All personal data obtained by virtue of the system, is processed fairly and lawfully and, in particular, will only be processed in the exercise of achieving the stated objectives of the CCTV System. In processing personal data, there is total respect for everyone's right to privacy.

8.2 The storage and security of the data will be strictly in accordance with the requirements of the DPA, the Information Commissioner's Code of Practice and the School's Data Protection Policy.

8.3 All data is processed in accordance with the principles of the DPA, which are set out in the Data Protection Policy.

8.4 Security measures are in place to prevent unauthorised or accidental access to, alteration, disclosure, or loss and destruction of information.

9. Maintenance of the CCTV System

9.1 Provision is made for regular/periodical service checks of the CCTV equipment, which includes cleaning of any all-weather domes or housings, checks on the functioning of the equipment, and any minor adjustments that need to be made to the equipment settings to maintain picture quality.

9.2 Key Personnel have full responsibility for all technical hardware aspects of the CCTV system. Should a fault develop, all cameras, servers, switches and computers have maintenance and warranty agreements in place.

9.3 Key Personnel will maintain appropriate records in respect of the functioning and maintenance of the cameras.

9.4 Key personnel will carry out monthly Planned Preventative Maintenance (PPM) checks on the CCTV software and equipment to ensure the system is functioning to required standards and no quality loss is evident.

10. Handling of recorded material

10.1 For the purposes of this policy 'recorded material' means any material recorded by, or as the result of, technical equipment which forms part of the CCTV system, but specifically includes images recorded digitally, on hard drive and by way of DVD copying, including digital video prints.

10.2 Subject to the equipment functioning correctly, images from the cameras are recorded throughout every 24-hour period.

10.3 Recorded footage is retained for a period of 30 Days.

10.4 Every digital recording obtained by using the CCTV System has the potential of containing recorded material, which may have to be admitted in evidence at some point during its life span. Irrespective of the format (e.g. DVD, paper copy, etc.), images

obtained from the CCTV system are treated strictly in accordance with this policy from the moment they are received until their final destruction.

10.5 Access to, and the use of, recorded material is strictly for the purposes defined in this policy.

10.6 Recorded material is not copied, sold, or used for commercial purposes or the provision of entertainment.

10.7 In complying with the DPA and GDPR 2018, it is intended, as far as reasonably practicable, to safeguard individual rights to privacy and ensure that the recorded material shall be processed lawfully and access restricted at all times.

10.8 The recorded material should not be viewed by anyone other than authorised personnel unless this is permitted by the Principal in consultation with the Data Protection Officer.

10.9 It may be beneficial to make use of 'real' digital recordings for the training and education of those involved in the operation and management of CCTV systems, and for those involved in the investigation, prevention, and detection of crime. Any material recorded by virtue of the CCTV system is only used for such training and education purposes.

10.10 A digital image is a copy of an image or images, which already exists on a hard drive or DVD. Digital images are not taken as a matter of routine. The Principal and/or Vice Principal, must authorise any requests to make digital images from the CCTV System. There must be a good reason for the request. If a digital image is made, the purpose of the request is recorded. The record will include brief details of the nature of the incident together with the location, time and date.

10.11 If a digital image is required in connection with a criminal investigation, it is treated as an exhibit and dealt with in accordance with the rules of evidence in respect of continuity, disclosure and any further requirements as set out by the police or prosecuting authority.

11. Copyright

11.1 Copyright and ownership of all material recorded by virtue of the CCTV System remains with the Data Controller.

12. Requests for access to records

12.1 The DPA 2018 provides that Data Subjects (individuals to whom ‘personal data’ relate) have a right to request data held about themselves, including those obtained by CCTV.

12.2 The Trust will not provide a copy of CCTV footage to anyone other than the police who make a request to assist with an ongoing investigation and insurers or their legal representatives who make a request as part of an investigation into an ongoing claim.

12.3 If an individual makes a right of access request including CCTV footage, they would not be entitled to receive a copy of the footage but may be invited to view the footage on site. This should be done by submitting a ‘CCTV Subject Access Form’ (Appendix 3) to the CCTV Key personnel, at the relevant school. Requests are carried out subject to conditions within 30 days of receiving such request.

12.4 If the Trust receives a request from an individual to view CCTV footage, then they will liaise with their Data Protection Officer who will balance the rights of the individual

requesting to view the footage against the rights of any other individuals who may be seen in the footage. A decision will be made on a case-by-case basis and communicated to the requester as soon as possible.

13. Public Information

13.1 A copy of this policy is made available on request.

13.2 Warning signs are in place at the academy in areas covered by the CCTV system. The signs indicate the presence of CCTV monitoring.

14. Complaints

14.1 Complaints and enquiries about the operation of CCTV within the academy should be directed to the Principal in the first instance.

15. Breaches of this policy

15.1 Any breach of this policy is initially investigated by the Principal, for the appropriate action to be taken.

Appendix A - Checklist

This CCTV system and the images produced by it are controlled by Great Heights Academy Trust who is responsible for how the system is used and for notifying the Information Commissioner about the CCTV system and its purpose (which is a legal requirement under GDPR and the Data Protection Act 2018).

The Academy has considered the need for using CCTV and have decided it is required to protect the building and its assets, to protect the health and safety of pupils, staff and visitors and to help detect, prevent and reduce incidence of criminal activity. 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.
An annual review of the use of CCTV is undertaken.

	Checked (Date)	By	Date of next review
Notification has been submitted to the Information Commissioner and the next renewal date recorded.			
There is a named individual who is responsible for the operation of the system.			
Staff named as CCTV authorised users have received appropriate training and received a copy of the school's CCTV Policy			
A system had been chosen which produces clear images which the law enforcement bodies (usually the police) can use to investigate crime and these can easily be taken from the system when required.			
Cameras have been sited so that they provide clear images.			
Cameras have been positioned to avoid capturing the images of persons not visiting the premises apart from reception where this is deemed appropriate and covered through signage.			
There are visible signs showing that CCTV is in operation. Where it is not obvious who is responsible for the system contact details are displayed on the sign(s).			
Images from this CCTV system are securely stored, where only a limited number of authorised persons may have access to them.			
The recorded images will only be retained long enough (i.e. longer than the recording system ordinarily records over) for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated.			
Except for law enforcement bodies, images will not be provided to third parties.			
The organisation knows how to respond to individuals making requests for copies of their own images. If unsure the controller knows to seek advice from the Information Commissioner as soon as such a request is made.			
Regular checks are carried out to ensure that the system is working properly and produces high quality images.			

Appendix B – CCTV Signage

It is a requirement under GDPR and the Data Protection Act 2018 to notify people entering a CCTV protected area that the area is monitored by CCTV and that pictures are recorded. The academy is to ensure that this requirement is fulfilled.

The CCTV sign must include the following:

- That the area is covered by CCTV surveillance and pictures are recorded
- The purpose of using CCTV
- The name of the academy
- The contact telephone number or address for enquiries

Appendix Three – CCTV Subject Access Request Form

This form is for any person who wishes to apply for access to CCTV footage held at a site of Great Heights Academy Trust only.

A separate form should be completed for each individual.

Section 1: Your Details (Please complete the form in black ink in block capitals)

Surname:	First Name:
Title:	Previous names:
Date of Birth:	Contact Number:
Current Address:	Previous Address(es):
Email address:	
Proof of ID: Two different documents as evidence of your name and current address (you can send copies of these through the post which will be securely destroyed once we have verified your identity; however we reserve the right to ask to see original documents); and If, requesting footage of yourself, a recent full face photograph of you so we can identify you in any CCTV images.	

Section 2: What footage are you requesting (please tick the relevant box)

Footage regarding myself	☐
Footage regarding some else	☐
Footage regarding others	☐

Section 3: Third parties details (only complete this section if you are requesting access to someone else's footage)

Surname:	First Name:
Title:	Previous names:
Date of Birth:	Contact Number:
Current Address:	Previous Address(es):
Email address:	

Please explain your relationship to this person (tick the relevant box below):

Mother	☐
Father	☐
Carer	☐
Other	☐

If you have selected other please explain:

Section 4: Details of the information you are requesting:

The camera location, date and time of the incident, and the nature of the incident: