Great Academies Education Trust

# CCTV Policy

| | |
|---|---|
| Prepared/reviewed by | Finance Director |
| Date | February 2025 |
| Approved by | Audit and Risk Committee |
| Date | February 2025 |
| Review date | January 2026 |

Great Academies Education Trust

CONTENTS PAGE

# Table of Contents

## 1. POLICY AIM

1.1 This document will enable staff of Great Academies Education Trust to comply with legislation relating to CCTV in all circumstances

1.2 The purpose of CCTV is to protect staff, students and the public, discourage aggressive and abusive behaviour, protect the Great Academies Education Trust infrastructure, and provide evidence where required to investigate complaints and incidents.

1.3 The policy will set out the purpose of using CCTV, what information will be recorded, who will have access to this information and how this information will be stored and disposed of.

## 2. POLICY STATEMENT

2.1. This Policy seeks to ensure that the Closed Circuit Television (CCTV) system used at Great Academies Education Trust is operated in compliance with the law relating to data protection (currently the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018 ("DPA 2018") and as amended from time to time) and includes the principles governing the processing of personal data as set out in Appendix 1. It also seeks to ensure compliance with privacy law. It considers best practice as set out in codes of practice issued by the Information Commissioner and by the Home Office. Great Academies Education Trust therefore uses CCTV only where it is necessary in pursuit of a legitimate aim, as set out in clause 2.2, and only if it is proportionate to that aim.

2.2. Great Academies Education Trust seeks to ensure, as far as is reasonably practicable, the security and safety of all students, staff, visitors, contractors, its property, and premises.

Great Academies Education Trust therefore deploys CCTV to:

- promote a safe Great Academies Education Trust community and to monitor the safety and security of its premises, staff, students and visitors.
- assist in the prevention, investigation, and detection of crime.
- assist in the apprehension and prosecution of offenders, including use of images as evidence in criminal proceedings; and
- assist in the investigation of breaches of its codes of conduct and policies by staff, students and contractors and where relevant and appropriate investigating complaints.

2.3 This policy will be reviewed annually to assess compliance with clauses 2.1 and 2.2 and to determine whether the use of the CCTV system remains justified.

## 3. SCOPE

3.1 This policy applies to CCTV systems in all properties of Great Academies Education Trust.

3.2 This policy does not apply to any Webcam systems located in meeting rooms, classrooms or lecture theatres operated by Faculties or ICT, which are used for the purposes of monitoring room usage and to assist with the use of the audio-visual equipment.

3.3 This policy applies to all Great Academies Education Trust staff, contractors and agents who operate, or supervise the operation of, the CCTV system including Senior Leadership, IT and estates staff, and the Data Protection Officer.

## 4. ROLES AND RESPONSIBILITIES

4.1 The Trust Data Protection Officer, with the support of School Data Protection Officers and Senior Leadership Teams, has the overall responsibility for this policy but has delegated day-to-day responsibility for overseeing its implementation to the staff identified in this policy. All relevant members of staff have been made aware of the policy and have received appropriate training.

4.2 The Data Protection Officer, with the support of the IT department, is responsible for ensuring that the CCTV system including camera specifications for new installations complies with the law and best practice referred to in clause 2.1 of this policy. Where new surveillance systems are proposed, the IT staff will consult with the Data Protection Officer to determine whether a data protection impact assessment is required.

4.3 Only the staff of IT department or a properly appointed maintenance contractor for Great Academies Education Trust CCTV system is authorised to install and/or maintain it.

4.4 The Data Protection Officer is responsible for the evaluation of locations where live and historical CCTV images are available for viewing. The list of such locations and the list of persons authorised to view CCTV images is maintained by the responsible person at each site.

4.5 Changes in the use of Great Academies Education Trust CCTV system can be implemented only in consultation with Great Academies Education Trust Data Protection Officer or the Great Academies Education Trust Legal Advisors.

4.6 Only authorised personnel shall have access to the CCTV system. In each individual academy this must be authorised by the Principal, and only approved where the access is in the spirit and confines of this policy.

## 5. SYSTEM DESCRIPTION – FIXED CAMERAS

5.1 The CCTV systems installed in and around Great Academies Education Trust estate cover building entrances, car parks, perimeters, external areas such as courtyards, internal areas such as social spaces, computer rooms, rooms with high value equipment, some corridors and reception areas. They continuously record activities in these areas.

5.2 CCTV cameras are not installed in areas in which individuals would have an expectation of privacy such as toilet cubicles, changing facilities etc.

5.3 CCTV cameras are installed in such a way that they are not hidden from view. Signs are prominently displayed where relevant, so that staff, students, visitors, and members of the public are made aware that they are entering an area covered by CCTV. The signs also contain contact details as well as a statement of purposes for which CCTV is used.

5.4 The contact point for queries about CCTV around **Great Academies Education Trust** should be available to staff, students, and members of the public during normal business hours. Any employees staffing the contact point must be familiar with this document and the procedures to be followed if an access request is received from a Data Subject or a third party.

## 6. COVERT RECORDING

6.1 Covert recording (i.e. recording which takes place without the individual's knowledge):

6.1.1 may only be undertaken in exceptional circumstances, for example to prevent or detect an unlawful act or other serious misconduct, and if is proportionate i.e., there is no other reasonable, less intrusive means of achieving those purposes;

6.1.2 may not be undertaken without the prior written authorisation of the Chief Executive Officer (CEO)**.** All decisions to engage in covert recording will be documented, including the reasons.

6.1.3 will focus only on the suspected unlawful activity or suspected serious misconduct and information obtained which is not relevant will be disregarded and where reasonably possible, deleted; and

6.1.4 will only be carried out for a limited and reasonable period consistent with particular purpose of the recording and will not continue after the investigation is completed.

## 7. OPERATING STANDARD

7.1 The operation of the CCTV system will be conducted in accordance with this policy.

7.2 Viewing of footage from an authorised machine and room:

7.2.1 No unauthorised access to the room ("the Control Room") will be permitted at any time during the viewing of footage. The Control Room may differ depending on the authorised staff member who is accessing the footage but should meet these specified requirements at the time the footage is being viewed.

7.2.2 Other than the staff member accessing the footage, access to the Control Room, during the viewing of the footage, will be limited to:

- persons specifically authorised by the Principal or CEO
- maintenance engineers.
- police officers where appropriate; and
- any other person with statutory powers of entry.

7.2.3 Monitors are not visible from outside the room.

7.2.4 Before permitting access to the Control Room, staff will satisfy themselves of the identity of any visitor and existence of the appropriate authorisation. All visitors are required to complete and sign the visitors' log, which includes details of their name,

department and/or the organisation that they represent, the person who granted authorisation and the times of entry to and exit from the Control Room.

7.2.5 A log of shall be retained on a secure shared drive setting out the following:

- person reviewing recorded footage.
- time, date, and location of footage being reviewed; and
- purpose of reviewing the recordings.

7.3 Processing of Recorded Images

7.3.1 CCTV images will be displayed only to persons authorised to view them or to persons who otherwise have a right of access to them. Where authorised persons access or monitor CCTV images on workstations, they must ensure that images are not visible to unauthorised persons for example by minimising screens when not in use or when unauthorised persons are present. Workstation screens must always be locked when unattended.

7.3.2 CCTV images and recordings will not be shared by email in any way.

7.4 Quality of Recorded Images

7.4.1 Images produced by the recording equipment must be as clear as possible, so they are effective for the purpose for which they are intended. The standards to be met in line with the codes of practice referred to clause 1 of these procedures are set out below:

- recording features such as the location of the camera and/or date and time reference must be accurate and maintained.
- cameras must only be situated so that they will capture images relevant to the purpose for which the system has been established.
- consideration must be given to the physical conditions in which the cameras are located i.e. additional lighting or infrared equipment may need to be installed in poorly lit areas;
- cameras must be properly maintained and serviced to ensure that clear images are recorded, and a log of all maintenance activities kept; and
- as far as practical, cameras must be protected from vandalism to ensure that they remain in working order. Methods used may vary from positioning at height to enclosure of the camera unit within a vandal resistant casing.

## 8. RETENTION AND DISPOSAL

8.1 CCTV images are not to be retained for longer than necessary, considering the purposes for which they are being processed. Data storage is automatically managed by the CCTV digital records which overwrite historical data in chronological order to produce an approximate 28-day rotation in data retention.

8.2 Provided that there is no legitimate reason for retaining the CCTV images (such as for use in disciplinary and/or legal proceedings), the images will be erased following the expiration of the retention period.

8.3 All retained CCTV images will be stored securely.

## 9. DATA SUBJECT RIGHTS

9.1 Recorded images, which directly or in combination with other factors enable a data subject to be identified, are considered to be the personal data of the individuals whose images have been recorded by the CCTV system.

9.2 Data Subjects have a right of access to the personal data under the GDPR and DPA 2018. They also have other rights under the GDPR and DPA 2018 in certain limited circumstances, including the right to have their personal data erased, rectified, to restrict processing and to object to the processing of their personal data.

9.3 Data Subjects can exercise their rights by submitting a request in accordance with the Great Academies Education Trust policies.

9.4 On receipt of the request, the Data Protection Officer, or their representative, will liaise with the Trust IT Manager regarding compliance with the request, and subject to clause 10.5, the Data Protection Officer will communicate the decision without undue delay and at the latest within one month of receiving the request from the Data Subject.

9.5 The period for responding to the request may be extended by two further months where necessary, considering the complexity and number of the requests. The Data Protection Officer will notify the Data Subject of any such extension within one month of receipt of the request together with reasons.

## 10. THIRD PARTY ACCESS

10.1 Third party requests for access will usually only be considered in line with the GDPR and DPA 2018 in the following categories:

- legal representative of the Data Subject.
- Legal representative of the trust
- law enforcement agencies including the Police.
- disclosure required by law or made in connection with legal proceedings; and
- HR or other staff responsible for employees and school or trust staff responsible for students in disciplinary and complaints investigations and related proceedings.

10.2 Legal representatives of the Data Subjects are required to submit to Great Academies Education Trust a letter of authority to act on behalf of the Data Subject along with appropriate proof of the Data Subject's identity.

10.3 The Data Protection Officer will disclose recorded images to law enforcement agencies including the Police once in possession of a form certifying that the images are required for either:

- an investigation concerning national security.
- the prevention or detection of crime; or
- the apprehension or prosecution of offenders

and that the investigation would be prejudiced by failure to disclose the information. Where images are sought by other bodies/agencies with a statutory right to obtain information, evidence of that statutory authority will be sought before CCTV images are disclosed.

10.4 Every CCTV image disclosed is recorded in the CCTV Operating Logbook and contains:

- the name of the police officer or other relevant person in the case of other agencies/bodies receiving the copy of the recording.
- brief details of the images captured by the CCTV to be used in evidence or for other purposes permitted by this policy.
- the crime reference number where relevant; and
- date and time the images were handed over to the police or other body/agency.

10.5 Requests of CCTV images for staff or student disciplinary purposes shall be submitted in writing to the Principal of the academy or the CEO in consultation with the Data Protection Officer.

10.6 Requests for CCTV information under the Freedom of Information Act 2000 will be considered in accordance with that regime.

## 11. COMPLAINTS PROCEEDURE

11.1 Any complaints relating to the CCTV system should be directed in writing to the Data Protection Officer promptly and in any event within 7 days of the date of the incident giving rise to the complaint. A complaint will be responded to within a month following the date of its receipt. Records of all complaints and any follow-up action will be maintained by the relevant office. If a complainant is not satisfied with the response, they may appeal to the CEO or the Trust Board.

11.2 Complaints in relation to the release of images should be addressed to the Data Protection Officer as soon as possible and in any event no later than three months from the event giving rise to the complaint.

## 12. USEFUL LINKS

The Information Commissioner's Code of Practice can be found at:

https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

## 13. RELATED POLICIES & STRATEGIES

- Data Protection Policy
- Complaints Policy
- Staff Disciplinary Policy and other staff related policies

# APPENDIX ONE: Procedures for staff viewing CCTV footage

**1. Access Control and Authentication**

1.1 Only authorised personnel with a legitimate reason for accessing CCTV footage will be granted permission.

1.2 Each staff member granted access will have a unique login and password for the CCTV system.

1.3 Login credentials must not be shared, and staff members must log out of the system when not actively monitoring footage.

1.4 Users will only access CCTV on approved devices which is not to include mobile phones or personal devices.

**2. Purpose of Viewing**

2.1 Staff members may only view CCTV footage for legitimate purposes, as documented in the CCTV policy.

2.2 Viewing of CCTV footage for personal or non-professional reasons is strictly prohibited.

**3. Recording and Documentation**

3.1 Before accessing CCTV footage, staff members must document the reason for viewing, including date, time, and the nature of the incident or concern.

3.2 Any actions taken as a result of viewing CCTV footage, such as reporting an incident, must be documented.

**4. Confidentiality and Data Sharing**

4.1 CCTV footage is considered confidential and must not be disclosed to unauthorised individuals.

4.2 Sharing of footage outside the academy trust is only permitted in compliance with data protection laws and regulations, and the CCTV policy.

4.3 CCTV footage and images must not be shared by email and should only be shared by storing in an authorised location which is secure and has a retention policy. This location can be established by checking with the relevant IT personnel.

**5. Monitoring Duration**

5.1 Staff members must only monitor CCTV footage for the necessary duration required to achieve the legitimate purpose for viewing.

5.2 Continuous, prolonged, or unnecessary monitoring is not allowed.

**6. Incident Reporting**

6.1 If staff members observe any suspicious or concerning activity while monitoring CCTV footage, they must promptly report it to the appropriate authorities or designated personnel.

6.2 All incidents reported must be documented, and the relevant authorities should be notified as appropriate.

**7. Technical Issues and Maintenance**

7.1 Staff members should report any technical issues with the CCTV system promptly to the designated IT support or maintenance personnel.

7.2 Routine checks and maintenance of CCTV equipment will be conducted to ensure optimal performance.

**8. Training and Awareness**

8.1 Staff members granted access to CCTV footage will undergo training on the responsible and ethical use of CCTV and the procedures outlined in this appendix.
8.2 Training will be provided periodically to ensure staff members are aware of any updates or changes to the CCTV procedures.

**9. Compliance Checks**
9.1 Random compliance checks will be conducted to ensure that staff members are adhering to the procedures outlined in this appendix.
9.2 Non-compliance will be addressed through appropriate measures, including additional training or disciplinary action if necessary.

Great Academies Education Trust

## APPENDIX TWO: CCTV recorded image access log

| CCTV access log | | | | | |
|---|---|---|---|---|---|
| **Authorised staff name** | **School** | **Date and time of recording** | **Reason for viewing** | **Further action taken (e.g., any images/recordings shared or saved)** | **Notes** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

## APPENDIX THREE: CCTV operator agreement

I confirm I have read and understood the CCTV Policy and agree to adhere by the rules of the policy as an operator of this system.

In addition, I will update the CCTV Recorded Image Access Log each time I access the system to review a recording. I will:

- record the reason for viewing any images.
- detail any retained images, why these were retained and diarise to review saved images for deletion.
- I will ensure any retained images are password protected.
- I understand images including retained images must not be shared with third parties, including staff who are not part of the senior leadership team.
- any shared images must have approval for sharing from the principal.

Name of authorised operator:

Full Name:

Signature:

Date:

School:

I confirm that is an authorised operator of the CCTV system.

Principal name:

Principal signature:

Date:

School:

## APPENDIX FOUR: CCTV log of authorised personnel

It is proposed that this log is maintained as a spreadsheet with these column headings. This document should be stored in a central secure location on the school shared drive with access restricted to authorised personnel.

| Name of authorised personnel | School name (or central team) | Date given access | Name of approver for access (Principal or CEO) | Date access removed (as required) |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Great Academies Education Trust

## APPENDIX FIVE: Site maps of cameras and signage

These maps should be added by the individual academy.