# ACCOMPLISH
# MULTI ACADEMY TRUST

# SURVEILLANCE AND CCTV POLICY

| | |
|---|---|
| **Date** | October 2024 |
| **Prepared by** | Trust |
| **Approved by** | Trust Board |
| **Review Date** | Annual from original policy date |
| **Version** | 1 |
| **Changes to document** | None |

**Version Control**

| Version | Revision Date | Revised By | Section Revised |
|---|---|---|---|
| | | | |

**CONTENTS**

## 1 STATEMENT OF INTENT

1.1 The policy sets our appropriate actions and procedures, which the Accomplish Multi Academy Trust (AMAT): must follow to comply with the Data Protection ACT 2018, General Data Protection Regulations (GDPR) guidelines (May 2018) and the Information Commissioner's Code of Practice in respect of the use of CCTV (Closed Circuit Television) surveillance systems currently and any future installation.

1.2 This document should be read in conjunction with the following related policies and procedures:

- Trust Data Protection Policy
- ICO Code of Practice
- Other policies and procedures relating to GDPR

1.3 The CCTV system includes internal and external remotely operated cameras and is used for the purpose of:

- Safeguarding of pupils/staff and visitors
- Security of the Trust's premises and assets
- Without prejudice, to protect the personal safety and property of pupils, staff and visitors
- To support the policy in preventing and detecting crime
- In a limited and restricted number of cases, to support insurance companies with possible claims

1.4 The CCTV system will not be used to:

- On an individual's right to privacy
- Monitor people in spaces where they have a heightened expectation of privacy (including toilets and changing rooms)
- Follow particular individuals, unless there is an ongoing emergency incident occurring
- Purpose any other purpose than the ones state above

1.5 The list of uses of CCTV is not exhaustive and other purposes may be or become irrelevant

1.6 The CCTV system is registered with the Information Commissioner's Office

**Registration number: Z2809737**

**Responsible Persons:** The Senior Leader responsible is Tracy Swinburne – Accomplish Trust CEO. The systems are supported by the Site Teams and Trust IT services with regard to networking and servers. The Site teams will work with suitable suppliers to provide maintenance and servicing where required.

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

1.8 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

1.9 The footage generated by the system should be of good enough quality to be of use to the police or court in identifying suspects

## 2 LEGAL FRAMEWORKS

2.1 This policy has due regard to legislation including, but not limited to, the following:

- The regulation of Investigatory Powers Act 2000
- The Protection of Freedom Act 2012
- The General Data Protection Regulation
- The Freedom of Information Act 2000
- 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 Children Act 1989
- The Children Act 2004
- The Equality Act 2010

2.2 This policy has been created with regard t the following statutory and non-statutory guidance:

- Home Office (2013) 'The Surveillance Camera Code of Practice'
- ICO (2018) General Data Protection Regulation (GDPR)
- ICO (2017) 'In the picture: A data protection code of practice for surveillance cameras and person information

## 3 DEFINITIONS

3.1 CCTV: Closed Circuit Television; video cameras used for surveillance

3.2 Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

3.3 Covert surveillance will only be used in extreme circumstances, such as where there is a suspicion of a criminal offence. If the situation arises where 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 in order to comply with data protection law

3.4 Cameras are located in places that require monitoring in order to achieve the aims of the CCTV system (as stated in section 1.1)

3.5 Cameras are located in some but not all AMAT buildings

3.6 Wherever cameras are installed appropriate signage is in place to warm members of the school community that they are under surveillance. The signage:

- Identifies the Trust/school as the operator of the CCTV system
- Identifies the school as the data controller
- Provides contact details for the Trust/school

3.7 Cameras are not and will not be aimed off school grounds into public spaces or people's private property

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

## 4 ROLES AND RESPONSIBILITIES

4.1 The **Trust Board** has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation is complied with.

4.2 The **Headteache**r must:

- Take responsibility for all day-today 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 the guidance set out in this policy is followed by all staff
- Review the CCTV policy to check that the school is compliant with the policy
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training in the use of the system and in data protection
- Sign off on an expansion or upgrading to the CCTV system, having taken advice from the DPO or delegate and taken into account the result of the data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure footage requests from third parties

4.3 The **Data Protection Officer** (DPO) or delegate must:

- Ensure training of persons with authorisation to access the CCTV system and footage in the use of the system and data protection
- Ensure training of all staff to recognise a subject access request
- Deal with subject access requests in line with the Freedom of Information Act (2000)
- 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)
- 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 trust/school, what their rights are, and how the trust/school will endeavour to protect their personal information
- Ensure that the CCTV systems are working properly and that the footage they produce is of hight quality so that individuals pictured in the footage can be identified
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces
- Ensure termly checks are carried out 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
- Review the CCTV policy to check that the trust is compliant with legislation

**4.4 The headteacher/site manager/ this in your schools**

- Take care of the day-to-day maintenance of operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws termly
- Ensure the data and time stamps are accurate termly

## 5 OPERATION OF THE CCTV SYSTEM

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

5.2 The system is registered with the Information Commissioner's Office

5.3 The system will not record audio

5.4 recording will have date and time stamps. This will be checked by headteacher/site manager termly and when clocks change

5.5 GDPR appropriate signage will be displayed in reception areas and entrance areas (of any outer buildings) to notify all users that CCTV is in operation, highlighting the trust as the operator and conveying the purpose of the system

## 6 STORAGE OF CCTV FOOTAGE

6.1 Footage will be retained for around 30 days depending on the technology in use within the schools. At the end of the retention period, the files will be overwritten automatically

6.2 On occasion footage may be retained for longer than 30 days, for example where a law enforcement body is investigating a crime, to give them the opportunity to view the images as part of an active investigation

6.3 Recording will be downloaded and encrypted, so that the data will be secure, and its integrity maintained, so that it can be used as evidence if required

6.4 The **Headteacher or delegate** will carry out termly checks to determine whether footage is being stored accurately, and being deleted after the retention period

## 7 ACCESS TO CCTV FOOTAGE

7.1 Access will only be given to authorised persons, for the purpose of pursuing the aims stated in section 1.1, or if there is a lawful reason to access the footage

7.2 Any individuals that access the footage must record their name, the date and time, and the reason for access in the access log

7.3 Any visual display monitors will be positioned so only authorised personnel will be able to see the footage

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

- Trust executive leaders
- The Headteacher
- Office Manager
- Anyone with express permission of the headteacher

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

7.6 All members of staff who have access will undergo training to ensure proper handling of the system and footage

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

7.8 CCTV footage will only be shared with a third party to further the aims of the CCTV system set out in section 1.1 (e.g. assisting the police in investigating a crime)

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

7.10 All requests for access should be set out in writing and sent to the Headteacher/CEO

7.11 The trust will comply with any court orders that grant access to the CCTV footage. The trust will provide the courts with the footage they need without giving them unrestricted access. The DPO will consider very carefully how much footage to disclose, and seek legal advice if necessary

7.12 The DPO will ensure that any disclosures that are made are done in compliance with IK GDPR

7.13 All disclosures will be recorded by the DPO

## 8 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

8.1 The trust follows the principle of privacy by design. Privacy is taken into account during every stage of the deployment of the CCTV system, including its replacement, development and upgrading

8.2 When the CCTV system is replace, developed or upgraded a DPIA will be carried out to be sure the aim of the system is still justifiable, necessary and proportionate

8.3 The DPO will provide guidance on how to carry out the DPIA. The DPIA will be carried out by the trust

8.4 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 put in place

8.5 A new DPIA will be done annually and/ or whenever cameras are moved, and/or new cameras are installed

## 9 SECURITY

9.1 The headteacher/site manager will be responsible for overseeing the security of the CCTV system and footage

9.2 The system will be checked for faults once a term

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

9.4 Footage will be stored securely and encrypted wherever possible

9.5 The CCTV footage will be password protected, and any camera operation equipment will be securely locked away when not in use

9.6 Proper cyber security measures will be put in place to protect the footage from cyber attacks

9.7 Any software updates (particularly security updates) published by the equipment's manufacturer that need to be applied, will be applied as soon as possible

## 10 MONITORING AND REVIEW

10.1 This policy will be monitored and reviewed on an annual basis by the trust

10.2 The trust will be responsible for monitoring changes to legislation that may affect this policy, and make the appropriate changes accordingly

10.3 The trust will communicate changes to this policy and all its schools for the Headteacher to communicate to all staff

**APPENDIX ONE**

**CCTV – USE AND DISCLORE OF IMAGES PROTOCOL**

Legitimate public concerns exist over the use of CCTV and may of the specific guidelines are designed to satisfy the community that the use of cameras is subject to adequate supervision and scrutiny. It is of fundamental importance that the public confidence is maintained by respecting individual privacy.

All employees that are authorised to view the CCTV images must read this protocol alongside the Surveillance and CCTV Policy and confirm that they understand and agree to abide by the policy and protocol.

CCTV images may only be viewed by authorised individuals. All authorised employees viewing the CCTV images will always act with utmost probity.

All images viewed by authorised employees must be treated as confidential. All authorised employees are to ensure that whilst viewing CCTV images, unauthorised employees or visitors cannot view the images.

All authorised employees are responsible to ensure that CCTV images are not left on any screen without an authorised employee being left in charge. An authorised employee should log out of the programme when leaving the screen.

Every viewing of the images will accord with the purposes and key objectives of the CCTV system and shall comply with the Surveillance and CCTV Policy.

A logged entry will be kept on record for every authorised viewing

Any breach of the Surveillance and CCTV Policy (or resulting data breach) will be dealt with in accordance with existing disciplinary policy and procedures. Individuals must recognise that any such breach may amount to gross misconduct, which could lead to dismissal.

Any breach of the UK-GDPR will be dealt with in accordance with that legislation. All authorised employees viewing CCTV images must be aware of their liability under this act.