THIS POLICY COVERS ALL ACADEMIES/SCHOOLS WITHIN ARDEN MULTI-ACADEMY TRUST

Name of Document	**CCTV Code of Practice**	
Lead	Martin Murphy, Chief Executive Officer	
Governor Committee	Business & Personnel Committee	
Policy Status	Draft	July 2012
	Trustee Approved	12th December 2023
Version No.	2	
Next Review	Autumn Term 2024	
Amendments	MPM reviewed on 10th June 2019	
	MPM reviewed February 2020	

1. Introduction

1.1 Arden Multi-Academy Trust (AMAT, the Trust) wishes to use Closed Circuit Television (CCTV) to protect against crime and to protect students, staff, parents and members of the public when they are on the school/academy premises.

1.2 Images of people captured on CCTV where they can be easily identified are defined as personal data under the Data Protection Act 2018. This means that the school/academy must meet the requirements of the act when using CCTV.

1.3 The Trust will have due regard to this policy to ensure that it can justify the use of CCTV under the Data Protection Act 2018 and subsequent guidance released by the Information Commissioner's Office and under the Human Rights Act 1998.

1.4 The policy applies where open use of CCTV is intended in public areas in and around the school/academy. It does not apply to targeted or covert surveillance activities. Any operation of this kind may only be carried out with reference to the Regulation of Investigatory Powers Act 2000 (RIPA) in consultation with the Council's Information Governance Team, RIPA office and/or the police. For further details see section 6.

1.5 This policy applies to all CCTV systems.

1.6 This policy will be reviewed regularly or as legal advice changes.

2. Responsibilities for CCTV operation

2.1 Responsibility for the administration and management of the CCTV Scheme in accordance with this policy lies with the Local Governing Body (LGB).

2.2 The LGB will appoint the Associate Headteacher to be responsible for:

- The appropriate lawful operation of the system;
- Ensuring all staff using the system have had a positive enhanced CRB check;
- The training of all staff involved in the use and operation of the system;
- The day-to-day compliance with the Data Protection Act, associated guidelines and with this policy;
- Notifying the Information Commissioner about the CCTV system;
- Annually updating the information sent to the Information Commissioner as required by the Data Protection Act 1998.

2.3 Precautions must be in place to control access to CCTV equipment and to prevent unauthorised access and misuse. All staff with access to the system must ensure that they adhere to any guidance or security precautions.

3. Legal basis for use Of CCTV Systems

3.1 The use of CCTV and the images recorded must comply with the Data Protection Act. The use of CCTV and images must be:

- Fairly and lawfully obtained;
- Adequate, relevant and not excessive;
- Accurate;
- Used only for purposes about which people have been informed;

- Secure and protected from unauthorised access;
- Not held longer than required for the purposes they were recorded (see para 5.5, p.4);
- Accessible to data subjects where a request has been made under the Data Protection Act and where the images are defined as personal data.

3.2 In order to use CCTV, the Trust must have a legitimate basis for recording the personal data. The legitimate purposes for which CCTV would be in use in Trust schools/academies include the following:

- Prevention and detection of crime, e.g., theft, arson and criminal damage;
- The protecton of the school/academy buildings and assets;
- Increasing the perception of safety and reduce the fear of crime;
- Protecting members of the public and private property;
- Ensuring the safety of students and others present on the school/academy premises.

3.3 The use of CCTV must be fair and must not be excessive or prejudicial to any individual or any group of individuals. In order for the use of CCTV to be fair, Trust schools/academies must inform people that CCTV is in use on its premises by means of notices.

3.4 The Human Rights Act 1998 (HRA) gives every individual a right to a private life and correspondence. This means that CCTV should not be used inappropriately and in areas where people could expect privacy. The HRA also requires that people are informed when CCTV is in operation.

In cases where schools within the Trust wish to video classroom activities, this should be done through consent to videoing forms signed by student's parents and not by using CCTV.

3.5 Trust schools/academies must document the purposes for which CCTV is to be used on the premises which are clarified in Section 1.1.

4. Ensuring that use Of CCTV is fair

4.1 Trust schools/academies should include the use of CCTV on the annual Data Protection Notification (registration) to the Information Commissioner's Office as one of the purposes for which it uses personal data.

4.2 Trust schools/academies must only use CCTV for the purposes it has stated. CCTV or images produced from it should not be used for any other purposes, particularly purposes which could not reasonably be envisaged by individuals.

4.3 Prior to installing a system, Trust schools/academies should consult with staff, parents and students about the use of CCTV on site and with any other nearby residents or business owners who may be affected by its use.

4.4 Trust schools/academies should ensure that students, staff and other people who use the buildings are informed of the use and purpose of CCTV. This is done by means of clear and obvious notices (A3 size) placed around school premises. Notices include the following information:

- The identity of the Data Controller;
- The purposes for which CCTV is being used, e.g., for the prevention or detection of crime or to increase safety and security while on the school/academy premises;
- Details of who to contact about the scheme and name/phone number where applicable.

4.5 The precise wording of a notice is:

- Warning: these premises are protected by closed circuit television. The images recorded are used for the purposes of crime prevention and public safety
  Operator:

SCHOOL NAME HERE	CONTACT NUMBER HERE

4.6 CCTV cameras are sited in such a way that they monitor the spaces that are intended to be covered by the equipment and are not focused on individuals. If a camera is sited near surrounding private property, this property is not visible on the transmitted/recorded images.

4.7 CCTV cameras are not positioned inside or overlooking teaching areas, including ICT suites. The AMAT is aware that the continuous videoing of individuals is considered to be directed surveillance under RIPA and is only likely to be justified in rare circumstances.

5. Selection, operation and maintenance of CCTV systems

Selecting a system

5.1 The CCTV system chosen is of sufficient quality to ensure that recordings and images produced are useable by Trust schools/academies and the police.
In general:

- Digital systems are recommended by the police as they provide good quality recordings and the capacity to produce clips and stills and to copy records to removable media.

- Equipment works effectively together. Consideration is required in relation to ensuring that a high quality digital CCTV system can only be used to its full capacity if the cameras are also of a similar quality.

- Equipment is maintained correctly checked regularly and repaired immediately if faulty, otherwise there is a risk that footage cannot be used in the investigation of a crime.

- Where removable media such as DVD or tape is used, it is of a high quality and replaced on a regular basis. Each item is identified by a unique mark and stored in date order where appropriate. Media is wiped completely before it is re-used.

- Cameras are sited so that individuals can be recognised easily, where required. Care is taken that the view from a camera does not become obscured.

All camera operatives are trained and only use the equipment for the purpose for which it was installed. Cameras, which are adjustable by the operator, are restricted so that the operator cannot adjust or manipulate the camera to overlook places that are not intended to be covered by the system.

Security

5.2 CCTV equipment capable of recording or downloading data is held in the control room in the IT office. Access is strictly confined to authorised staff. Where other staff or visitors need to have access to the system, this is documented.

The Site Team also have access to the CCTV images for safeguarding and site security purposes. This is live feed only and does not allow data recording.

5.3 All tapes/disks are clearly labelled with the date, start time of recording and location of the camera.

5.4 Once tapes/disks have been labelled they must be stored securely; only named persons shall have access to the tapes/disks.

5.5 If out of hours emergency maintenance is required the staff member in charge of the CCTV system must be satisfied of the identity of contractors before allowing access to the equipment.

Retention of recordings

5.5 Recordings are held for a limited length of time and must be destroyed when their use is no longer required. This should be for a maximum period of 28 days but this may be extended where the recordings are required for an ongoing investigation. When the retention period has been reached, digital recordings or removable media should be destroyed or wiped securely.

6. Covert Surveillance

6.1 On the rare occasions when Trust schools/academies may wish to use CCTV covertly (i.e., without making people aware of it), an application will be made under the Regulation of Investigatory Powers Act (RIPA). An application form will need to be completed and approved by the appropriate authorised senior person.

6.2 Where the police wish to undertake convert surveillance, they will be responsible for gaining authorisation.

7. Procedures for disclosure of CCTV records to other organisations

7.1 Access to CCTV recordings is initially restricted to the Chief Executive Officer/Associate Headteacher. Any third party access is allowed only after agreement from the Chief Executive Officer/Associate Headteacher and full details must be recorded in writing. Any persons requiring access to recordings or information must complete a CCTV data request form -** See appendix 1

7.2 CCTV recordings will be held only by the Trust unless there is a legitimate reason to disclose them. Disclosure includes the viewing of images by someone who is not the operator of the system as well as the transfer of recordings to another organisation.

7.3 Disclosure of the images to third parties should be limited including:

- The police, for the prevention and detection of crime
- A court for legal proceedings
- A solicitor for legal proceedings
- To comply with the Data Protection Act

7.4 Where recordings have been disclosed or viewed by an authorised third party the Trust must keep a record of:

- When the images were disclosed;
- Why they have been disclosed;
- Any crime incident number to which they refer;
- Who the images have been viewed by or disclosed to
- The outcome, if any, of the viewing or disclosure;
- The date/time the images were returned to the storage area or further details if the images are retained for evidential purposes.

7.5 Viewing of CCTV recordings by the police must be recorded in writing. Requests by the police are actioned under section 29 of the Data Protection Act. The police should provide a completed section 29 form stating that the information is required for the prevention and detection of crime. If a form is not available, or in an emergency, the Trust must record in writing when and why the information has been released.

7.6 Should a recording be required as evidence, a copy may be released to the police. Where this occurs the recording will remain the property of the AMAT. The date of the release and the purpose for which it is to be used must be recorded.

7.7 The police may require Trust schools/academies to retain recordings for possible use as evidence in the future. Such records must be stored and indexed so that they can be retrieved when required.

7.8 Applications received from other outside bodies (e.g., solicitors) to view or release tapes will be referred to the Chief Executive Officer. In these circumstances, tapes may be released where satisfactory evidence is produced showing that they are required or legal proceedings, an information access request (see section 8) or in response to a court order.

7.9 Recorded images must not be made widely available (e.g. they should not be available to the media or placed on the internet).

8. Subject access requests

8.1 Under section 7 of the Data Protection Act 1998, individuals who are the subject of personal data are entitled to request access to it. This includes CCTV images where they are defined as personal data within the meaning of the Act.

8.2 Recent legal cases have raised the issue of when CCTV images should be considered as personal data. Guidance arising from this implies that personal data must be substantially about the person and should affect their privacy in some way. In relation to CCTV this will

not include all images.

A wide shot of, for example, a playground or the school corridors with many people in view of the cameras would not normally be considered as the personal data of all those involved. However, where a camera has picked up an individual or group of individuals specifically, or has been moved to zoom in on them, the images recorded can be considered personal data.

8.3 Where a request has been made to view an image or recording, an application must be made in writing to the Chief Executive Officer/Associate Headteacher. The individual may wish to access either a still image or part of a recording. Where third parties are included in the shots, they should be removed where this is technically possible. Where removal is not possible, their consent should be sought. Where consent is refused or where it is not possible to gain consent, a balanced decision needs to be made, taking conflicting interests into account, as to whether it is reasonable in all circumstances to release the information to the individual.

8.4 There is no obligation to provide information where a request has been made after CCTV records have been routinely destroyed in accordance with this policy - see 5.5 (i.e. for recordings that no longer exist). However, where a request has been made for recordings still in existence, they must not be destroyed until the request is complete.

8.5 For further information on dealing with requests under the Data Protection Act, AMAT Data Protection policies should be consulted.

9. Breaches of policy

9.1 Any breach or alleged breach of this policy or the Trust guidelines on the use of CCTV by the school/academy staff or other individuals should be investigated by an appropriate representative of the Senior Leadership Team or, in the case of the Chief Executive Officer, by a member of the Trust Board.

9.2 An investigation should be carried out into any breaches of policy and procedures reviewed or put in place to ensure that the situation does not arise again.

9.3 Where there is evidence that an employee of the Trust has breached this policy they may be subject to disciplinary action.

10. Complaints

10.1 Any complaints about the operation of the CCTV system should be addressed to the Chief Executive Officer where they will be dealt with according to the Trust standard complaints procedures, with reference to this policy.

11. Further Information

Further information is available from the Information Commissioner on 01625 545 745 or http://www.informationcommissioner.gov.uk

** *Appendix 1* *Arden Multi-Academy Trust: CCTV SYSTEM*

Data Protection Act, 1998

How to apply for access to information held on the CCTV system

These notes explain how you can find out what information, if any, is held about you on the CCTV system.

PLEASE NOTE THAT VIDEO IS RETAINED FOR A MAXIMUM OF 28 DAYS.

Your Rights

Subject to certain exemptions, you have a right to be told whether any personal data is held about you. You also have a right to a copy of that information in a permanent form except where the supply of such a copy is not possible or would involve disproportionate effort or if you agree otherwise. ---------- will only give that information if it is satisfied with your identity. If release of the information will disclose information relating to (an)other individual(s), who can be identified from that information, ---------- is not obliged to comply with a data access request unless

- The other individual(s) has/have consented in writing to the disclosure of the information, or
- It is reasonable in all circumstances to comply with the request without the consent of the other individual(s).

---------- Rights

---------- may deny access to information where the Data Protection Act (the Act) allows. The main exemptions in relation to information held on the CCTV System are where the information may be held for:

- the prevention and detection of crime or
- the apprehension and prosecution of offenders

and giving you the information may be likely to prejudice any of these purposes.

Our Aim

We aim to respond and/or supply the information within 28 days after receiving your request, the fee, proof of identity and sufficient information to help locate the information you require.

THE APPLICATION FORM: ALL sections of the form must be completed. Failure to do so may delay your

application.

Section 1 Asks you to give information about yourself that will help ---------- to confirm your identity. ---------- has a duty to ensure that the information it holds is secure and it must be satisfied that you are who you say you are.

Section 2 Asks you to provide evidence of your identity by producing **TWO** official documents, which between them clearly show your name, date of birth and current address.

A recent, full face photograph of yourself must also be provided
BUT ONLY IF YOU ARE THE SUBJECT OF THE CCTV SEARCH

Section 3 Full details of the incident.

Section 4 The declaration must be signed by you.

When you have complete and checked this form, take or send it together with the required TWO identification documents, photograph and fee to:

The CCTV Operations Manager, ----------,

----------, ----------, ----------

SECTION 1: About yourself

The information requested below is to help Arden Multi-Academy Trust to satisfy itself as to your identity and to find any data held about you.

PLEASE USE BLOCK LETTERS

Title (Mr, Mrs, Miss, Ms, Dr, Rev, others)……..

Full name……..

Full address…….

……..…

……

……

……Post Code……

Date of birth…….

Place of birth……..

Sex (male/female)……..

Telephone numbers – home/office……..

Mobile…….

Section 2: Proof of identity

To help establish your identity your application must be accompanied by **TWO** official documents that, between them, clearly show your name, date of birth and current address.

For example: a birth/adoption certificate, driving license, medical card, passport or other official document that shows your name and address.

A recent, full face photograph of yourself must also be provided
BUT ONLY IF YOU ARE THE SUBJECT OF THE CCTV SEARCH.

Failure to provide the above proof of identity and photograph may delay your application.

SECTION 3: To help us find the information

If the information you have requested refers to a specific offence or incident, please complete this section.

Please complete a separate box in respect of different categories/incidents/involvement. Continue on a separate sheet if necessary

If the information you require relates to a vehicle, property, or is another type of information not specified so far, please complete the relevant section.

Were you: *(tick box below)*

A person reporting an offence or incident	
A witness to an offence or incident	
A victim of an offence	
A person accused or convicted of an offence	

OTHERS – Please explain……

……

……

……

Date(s) of incident……..

Time(s) of incident……..

Location of incident……..

……

……

……

……

Details of incident……..

……

……

……

……

……

……

……

Section 4: Declaration

DECLARATION (to be signed by the applicant)

The information that I have supplied in this application is correct and I am the person to whom it relates.

Signature……..Date……..

Warning – a person who makes a false declaration or impersonates or attempts to impersonate another may be guilty of an offence.

PLEASE CHECK

- **ALL** sections on this form are completed?
- **TWO** identification documents enclosed?
- Recent, full face photograph of yourself enclosed? **(only if appropriate)**

Further information:

These notes are only a guide. The law is set out in the Data Protection Act, 1998, obtainable from the school office. Further information and advice may be obtained from:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 08456 306060 or 01625 545745 **Email: mail@ico.gsi.gov.uk**

Please note that this application for access to information must be made direct to ---------- (address on page 1) and **NOT** to the Information Commissioner's Office.

OFFICIAL USE ONLY

Please complete ALL of this section (refer to 'CHECK' box above).

Application checked and legible?		**Date application received**	
Identification documents checked?			

Details of 2 documents (see Section 2)

Member of staff completing this section:

Name		Position	
Signature		Date	