



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

| | | |
|---------------------------|---------------------------------|--------------------------------|
| Name of Policy | CCTV Policy | |
| Lead | Martin Murphy, CEO | |
| Governor Committee | Business & Personnel Committee | |
| Policy Status | Draft | July 2012 |
| | Trustee Approved | 10 th December 2024 |
| Version No. | 2 | |
| Next Review | Autumn Term 2025 | |
| Amendments | Reviewed by MPM – February 2020 | |
| | | |
| | | |
| | | |



Introduction

- The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system at the school/academy.
- The system comprises a number of fixed and dome cameras located around the school/academy site.
- All cameras in our schools/academies are monitored from a central control room, reception, pastoral offices and site team office and are only available to selected staff.
- This Code follows General Data Protection Regulation (GDPR) guidelines.
- The Code of Practice will be subject to review bi-annually to include consultation as appropriate with interested parties.
- The CCTV system is owned by the school/academy.

1. Objectives of the CCTV scheme

- To protect the school/academy buildings and their assets
- To increase personal safety and reduce the fear of crime
- To support the police in a bid to deter and detect crime
- To assist in identifying, apprehending and prosecuting offenders
- To protect members of the public and private property
- To assist in managing the school/academy

2. Statement of intent

- The CCTV Scheme will be registered with the Information Commissioner under the terms of the General Data Protection Regulation (GDPR) and will seek to comply with the requirements both of the General Data Protection Regulation (GDPR) and the Commissioner's Code of Practice.
- The school/academy will treat the system and all information, documents and recordings obtained and used as data which are protected by General Data Protection Regulation (GDPR).
- Cameras will be used to monitor activities within the school/academy and its car parks and other public areas to identify criminal activity actually occurring, anticipated, or perceived, and for the purpose of securing the safety and well-being of the school/academy, together with its visitors.
- Staff have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.
- Unless an immediate response to events is required, staff must not direct cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the school/academy 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. Data will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. Data will never be released to the media for purposes of entertainment.
- The planning and design has endeavoured to ensure that the scheme 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.

3. Operation of the system

- The Scheme will be administered and managed by the Governing Body, in accordance with the principles and objectives expressed in the code.
- The day-to-day management will be the responsibility of the Senior Leadership Team, Site Manager and Network Manager during the day and the site team out of hours and at weekends.
- The control room will only be staffed by the Network Manager and IT team.
- The CCTV system will be operated 24 hours each day, every day of the year.

4. Control Room

- The Network Manager will check and confirm the efficiency of the system and in particular that the equipment is properly recording and that cameras are functional.
- Access to the CCTV control room will be strictly limited to the SMT, pastoral managers and Network Manager/IT team.
- Unless an immediate response to events is required, staff in the CCTV Control Room must not direct cameras at an individual or a specific group of individuals.
- Visitors and other contractors wishing to enter the control room will be subject to particular arrangements as outlined below.
- Control room operators must satisfy themselves over the identity of any other visitors to the control room and the purpose of the visit. Where any doubt exists access will be refused. It is vital that operations are managed with the minimum of disruption. Casual visits will not be permitted. Visitors must first obtain permission from the Network Manager, or his/her deputy and must be accompanied by him throughout the visit.
- Any visit may be immediately curtailed if prevailing operational requirements make this necessary.
- If out of hours emergency maintenance arises, the control room operators must be satisfied of the identity and purpose of contractors before allowing entry.
- For safeguarding purposes and health & safety requirements the site team have access to the

CCTV cameras in the site office to monitor movement of visitors and vehicles coming and going from the school site. This is live data feed only and cannot be downloaded or recorded. Downloading data can only be undertaken in the control room. The site team must ensure that when leaving the site office it is locked and the PC displaying the CCTV images is shut down or the screen is locked with a password.

- There must always be at least one control room operator present within the control room out of hours and weekends or the control room must be locked **OR** the control room must be locked. During the working day when not manned the room must be kept secured.
- Other administrative functions will include maintaining video data and hard disc space, filing and maintaining occurrence and system maintenance logs.
- Emergency procedures will be used in appropriate cases to call the emergency services.

5. Liaison

- Liaison meetings may be held with all bodies involved in the support of the system.

6. Monitoring Procedures

- Camera surveillance may be maintained at all times.
- A monitor is installed in the control room to which pictures will be continuously recorded.
- Pictures will be continuously recorded or when activated by movement.

7. Video Files Procedures

- In order to maintain and preserve the integrity of the data 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:
 - CCTV footage are date and time stamped
 - Data may be viewed by the police for the prevention and detection of crime.
 - Should CCTV footage be required as evidence, a copy may be released to the police under the procedures described previously in this code. Data will only be released to the police on the clear understanding that the footage remains the property of the school/academy, and both the video file and information contained on it are to be treated in accordance with his code. The school/academy also retains the right to refuse permission for the police to pass to any other person the CCTV footage file or any part of the information contained therein.
 - The police may require the school/academy to retain the stored data for possible use as evidence in the future. Such data will be properly indexed and properly and securely stored until they are needed by the police.
 - Applications received from outside bodies (e.g. solicitors) to view or release data will be referred to the Chief Executive Officer. In these circumstances data will normally be released where satisfactory documentary evidence is produced showing that they are required for legal proceedings, a subject access request, or in response to a court order. A fee can be charged in such circumstances: £10 for

subject access requests; a sum not exceeding the cost of materials in other cases.

- Any recorded CCTV footage is removed after 28 days.

8. Breaches of the code (including breaches of security)

- Any breach of the code of practice by school/academy staff will be initially investigated by the Chief Executive Officer, in order for him/her to take the appropriate disciplinary action.
- 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.

9. Assessment of the scheme and code of practice

- Performance monitoring, including random operating checks, may be carried out by the SLT.

10. Complaints

- Any complaints about the school/academy's CCTV system should be addressed to the Governing Body of each school.
- Complaints will be investigated in accordance with Section 9 of this code.

11. Access by the data subject

- The General Data Protection Regulation (GDPR) provides data subjects (individuals to whom "personal data" relate) with a right to data held about themselves, including those obtained by CCTV.

- Requests for data subject access should be made on an application form available on the CCTV Code of Practice document (Appendix1).

12. Public information

- Copies of this policy will be available to the public from the school/academy office and the Associate Headteacher.

Summary of key points:

- This policy will be reviewed every two years.
- The CCTV systems are owned and operated by each school/academy.
- The control room is locked when not be manned out of school hours.
- The control room is not open to visitors except by prior arrangement and good reason.
- Liaison meetings may be held with the police and other bodies.
- Recording data will be used properly indexed, stored and destroyed after appropriate use.
- Data may only be viewed by authorised staff, control room staff and the police.
- Data required as evidence will be properly recorded witnessed and packaged before copies are released to the police.
- Data will not be made available to the media for commercial or entertainment.
- Data will be disposed of securely.
- Any breaches of this code will be investigated by the Associate Headteacher. An independent investigation will be carried out for serious breaches.
- Breaches of the code and remedies will be reported to the Chief Executive Officer.