BDMAT
Birmingham Diocesan
Multi-Academy Trust

BDMAT
CCTV Policy

Issued: November 2022

Reviewed: Autumn 2024

Next review Date: Autumn 2027

1.0 Aims

This policy aims to set out the school's approach to the operation, management and usage of surveillance and closed-circuit television (CCTV) systems on school property.

1.1 Statement of intent

The purpose of the CCTV system is to:

- Make members of the school community feel safe
- Protect members of the school community from harm to themselves or to their property
- Deter criminality in the school
- Protect school assets and buildings
- Assist police to deter and detect crime
- Determine the cause of accidents
- Assist in the effective resolution of any disputes which may arise in the course of disciplinary and grievance proceedings
- To assist in the defense of any litigation proceedings

The CCTV system will not be used to:

- Encroach 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
- Pursue any other purposes than the ones stated above

The list of uses of CCTV is not exhaustive and other purposes may be or become relevant.

CCTV systems must be registered with the Information Commissioner under the terms of the Data Protection Act 2018. The system complies with the requirements of the Data Protection Act 2018 and UK GDPR.

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

Any 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.

2.0 Relevant legislation and guidance

2.1 Legislation

UK General Data Protection Regulation
Data Protection Act 2018
Human Rights Act 1998
European Convention on Human Rights
The Regulation of Investigatory Powers Act 2000
The Protection of Freedoms Act 2012
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 School Standards and Framework Act 1998
The Children Act 1989
The Children Act 2004
The Equality Act 2010

2.2 Guidance

Surveillance Camera Code of Practice (2021)

3.0 Definitions

- Surveillance: the act of watching a person or a place
- CCTV: closed circuit television; video cameras used for surveillance
- Covert surveillance: operation of cameras in a place where people have not been made aware they are under surveillance

4.0 Covert surveillance

Covert surveillance will only be used in extreme circumstances, such as where there is suspicion of a criminal offence. If the situation arises where covert surveillance is needed, the proper authorisation forms from the Home Office will be completed and retained.

5.0 Location of the cameras

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

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

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

5.3 Cameras are not and will not be aimed off school grounds into public spaces or people's private property. Cameras are positioned in order to maximise coverage, but there is no guarantee that all incidents will be captured on camera.

6.0 Roles and Responsibilities

6.1 The Local Academy Body

The governing board has the ultimate responsibility for ensuring the CCTV system is operated within the parameters of this policy and that the relevant legislation (defined in section 2.1) is complied with.

6.2 The Data Protection Officer

- Train 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
- 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 school, what their rights are, and how the school will endeavour to protect their personal information
- Ensure that the CCTV system is not infringing on any individual's reasonable right to privacy in public spaces

6.3 The Headteacher

- Take responsibility for all day-to-day 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 legislation
- Ensure all persons with authorisation to access the CCTV system and footage have received proper training from the DPO in the use of the system and in data protection

- Sign off on any expansion or upgrading to the CCTV system, after having taken advice from the DPO and taken into account the result of a data protection impact assessment
- Decide, in consultation with the DPO, whether to comply with disclosure of footage requests from third parties
- Receive and consider requests for third-party access to CCTV footage

6.4 The Head of IT

- Take care of the day-to-day maintenance and operation of the CCTV system
- Oversee the security of the CCTV system and footage
- Check the system for faults and security flaws
- Ensure the data and time stamps are accurate
- Train persons with authorisation to access the CCTV system and footage in the use of the system and in data protection
- Ensure that the CCTV systems are working properly and that the footage they produce is of high quality so that individuals pictured in the footage can be identified

7.0 Operation of the CCTV system

The CCTV system will:

- Be operational 24 hours a day, 365 days a year
- Be registered with the Information Commissioner's Office
- Not record audio
- Have date and time stamps. This will be checked by the system manager termly and when the clocks change
- Not use biometric monitoring software, such as facial recognition

8.0 Storage of CCTV footage

8.1 Footage will be retained for a maximum of 30 days. At the end of the retention period, the files will be overwritten automatically.

8.2 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.

8.3 Recordings 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.

8.4 The DPO will carry out routine checks to determine whether footage is being stored accurately, and being deleted after the retention period.

9.0 Access to CCTV footage

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.

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

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

9.1 Staff access

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

- The Executive Leadership Team
- The Head of School Support
- The Head of IT
- The Headteacher
- Anyone with express permission of the Executive Leadership Team or Headteacher

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

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

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

9.15 Staff without automatic access (those listed above) can request access to specific CCTV footage by submitting a request to the IT helpdesk. The request will be reviewed and approved by the Head of School Support, Head of IT and either Deputy CEO or Headteacher.

9.2 Subject access requests (SAR)

9.21 According to UK GDPR and DPA 2018, individuals have the right to request a copy of any CCTV footage of themselves.

9.22 Upon receiving the request the school will immediately issue a receipt and will then respond within 30 days during term time. The school reserves the right to extend that deadline during holidays due to difficulties accessing appropriate staff members.

9.23 All staff have received training to recognise SARs. When a SAR is received staff should inform the DPO in writing. When making a request, individuals should provide the school with reasonable information such as the date, time and location the footage was taken to aid school staff in locating the footage.

9.24 On occasion the school will reserve the right to refuse a SAR, if, for example, the release of the footage to the subject would prejudice an ongoing investigation.

9.25 Images that may identify other individuals need to be obscured to prevent unwarranted identification. The school will attempt to conceal their identities by blurring out their faces, or redacting parts of the footage. If this is not possible the school will seek their consent before releasing the footage. If consent is not forthcoming the still images may be released instead.

9.26 The school reserves the right to charge a reasonable fee to cover the administrative costs of complying with an SAR that is repetitive, unfounded or excessive.

9.27 Footage that is disclosed in a SAR will be disclosed securely to ensure only the intended recipient has access to it.

9.28 Records will be kept that show the date of the disclosure, details of who was provided with the information (the name of the person and the organisation they represent), and why they required it.

9.29 Individuals wishing to make an SAR can find more information about their rights, the process of making a request, and what to do if they are dissatisfied with the response to the request on the ICO website.

9.3 Third-party access

9.31 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).

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

9.33 All requests for access should be set out in writing and sent to the headteacher and the DPO.

9.34 The school will comply with any court orders that grant access to the CCTV footage. The school 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.

9.35 The DPO will ensure that any disclosures that are made are done in compliance with UK GDPR.

9.36 All disclosures will be recorded by the DPO.

10.0 Data protection impact assessment (DPIA)

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

10.2 The system is used only for the purpose of fulfilling its aims (stated in section 1.1).

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

10.4 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.

10.5 A new DPIA will be done annually whenever significant changes are made to the CCTV system, such as installing new camaras.

10.6 If any security risks are identified in the course of the DPIA, the school will address them as soon as possible.

11.0 Security

11.1 The Head of IT will be responsible for overseeing the security of the CCTV system and footage

11.2 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

11.3 Footage will be stored securely and encrypted wherever possible

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

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

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

12.0 Complaints

Complaints should be directed to the Headteacher or the DPO and should be made according to the school's complaints policy.

13.0 Monitoring

The policy will be reviewed annually by the DPO to consider whether the continued use of a surveillance camera remains necessary, proportionate and effective in meeting its stated purposes.

14.0 Links to other policies

- GDPR policy
- IT Security and Acceptable Use Policy
- Privacy notices for parents, pupils, staff, governors and suppliers
- Safeguarding policy