Beacon Academy Trust

A COMPELLING VISION FOR SUCCESS

CCTV POLICY

Approving Body	Trust
Date of Approval	April 2019
Due for Review	April 2022
Statutory (Y/N)?	N
Responsible Officer	BMAT CEO, for and on behalf of the Trust

I.PURPOSE AND LEGISLATIVE CONTEXT

1. BMAT is committed to the safety of its students, employees and visitors. The use of CCTV in line with this Policy forms part of this commitment. Specifically, this Policy aims to:

a. Ensure that CCTV recordings are only accessed or used when appropriate, in line with procedural and legal requirements;
b. Assist the management of BMAT and its constituent schools;
c. Protect BMAT premises and assets from physical damage;
d. Increase personal safety and reduce instances of aggression or crime;
e. Support investigations of known or suspected instances of inappropriate behaviour, aggression or physical damage. This may include investigations by the police when criminal activity is suspected; and
f. Assist with the identification, apprehension and prosecution of offenders.

2. This Policy has been drafted with due regard to the requirements of legislation and statutory guidance, including but not limited to:

a. The Data Protection Act 2018;
b. The Regulation of Investigatory Powers Act 2000;
c. Information Commissioner's Office Code of Conduct for CCTV;
d. The Freedom of Information Act 2000 and the Freedom of Information and Data Protection Regulations 2004;
e. The Equality Act 2010;
f. The Protection of Freedoms Act 2012;
g. The Children Act 1989 and the Children Act 2004;
h. The Education (Pupil Information) (England) Regulations 2005, as amended;
i. Article 8 of the Human Rights Act 1998;

3. This Policy operates alongside the following BMAT policies, which are available on the BMAT website:

a. Student Behaviour;
b. Employee Code of Conduct;
c. Security; and
d. Safeguarding and Child Protection.

4. The BMAT CCTV System will be managed in line with the following data protection principles. Data collected by the BMAT CCTV System will be:

a. Processed *lawfully, fairly and transparently*.
b. Collected for *legitimate purposes* only, as specified by this Policy and guided by relevant legislation or guidance;
c. Limited to what is *necessary and proportionate* to the legitimate purposes;
d. *Accurate, up to date* and destroyed if it is not accurate or up to date;
e. Stored in line with the BMAT Data Protection Policy, the BMAT Data Retention Schedule and data protection legislation or guidance;
f. *Processed securely* and not lost, destroyed, damaged or processed in an unauthorised way.

5. Monitoring and review: This Policy will be reviewed by the BMAT Trust Executive at least every three years. Advice will be sought from the BMAT DPO as appropriate.

6. Employee Conduct: BMAT employees are strongly advised to consider the importance of the right to privacy, of the integrity of personal data, and of the right not to be discriminated against because of a protected characteristic. If BMAT employees use or access CCTV equipment or footage in a way that goes against these rights or values, they will be sanctioned in line with the BMAT Disciplinary Policy. External agencies will be informed as appropriate, including the police in extreme cases.

II. LOCATION OF CCTV CAMERAS

7. The BMAT CCTV system operates 24 hours a day, every day of the year.

8. Where CCTV cameras are located: BMAT uses CCTV cameras to monitor activity in key areas of its premises, including corridors, entranceways, car parks and other public areas. This is to:

a. Identify known or suspected instances of aggression or crime;
b. Secure the safety and well-being of students, employees and visitors.

9. Where CCTV cameras are not located:

a. BMAT does not use CCTV cameras in class rooms, offices, meeting rooms or in areas where there is an increased expectation of privacy.
b. BMAT does not use CCTV cameras to record activity on private property (e.g. homes and gardens in the surrounding community).

10. Signage/Notices: Prominent notices, as required by the ICO Code of Practice for CCTV use, are located at all access routes to areas monitored by CCTV cameras.

11. Forbidden use of CCTV cameras:

a. CCTV cameras must not be used to conduct covert surveillance (whereby subjects are not informed) and BMAT does not have the authorisation to conduct covert surveillance.

b. Unless an immediate response to an incident is required, CCTV cameras must not be directed or targeted at individuals, their property or a specific group of individuals, unless authorisation is obtained using the Home Office Application Form for Directed Surveillance. If granted, authorisation will last for up to 3 months.

c. CCTV cameras must not be used for any purpose other than those set out in this Policy and in relevant legislation or statutory guidance.

d. Access to CCTV footage must be in line with Section IV of this Policy.

12. CCTV Control Rooms. Monitors are installed in CCTV control rooms, to which pictures are continuously recorded. CCTV control rooms are located at the:

a. Beal High School Upper Site;

b. Beal High School Lower Site;

c. Beal Sixth Form;

d. Forest Academy; and

e. Beacon Business Innovation Hub.

III. MANAGEMENT OF THE BMAT CCTV SYSTEM

13. For the purposes of this Policy, BMAT is the data controller (i.e. an individual or organisation that determines the purposes and the means of processing personal data). The data controller is responsible for ensuring that CCTV footage is recorded and processed legally, fairly, proportionately and for legitimate purposes.

a. The BMAT Trust Executive and Board of Trustees have overall responsibility for overseeing the use of the BMAT CCTV System in line with this Policy and relevant legislation or guidance.

b. BMAT School Principals have overall responsibility for overseeing the use of the BMAT CCTV System at a school level, in line with this Policy and relevant legislation or guidance.

14. BMAT Trustees, members of the BMAT Trust Executive and BMAT School Principals should seek advice from the BMAT Data Protection Officer, as appropriate.

15. The BMAT Data Protection Officer is responsible for implementing the BMAT Data Protection Policy and dealing with freedom of information requests or subject access requests in line with that Policy and with data protection legislation or guidance. In relation to the BMAT CCTV System, the BMAT Data Protection Officer is responsible for ensuring that:

a. The BMAT CCTV System is registered with the ICO;
b. The installation of any additional CCTV equipment is subject to a Data Protection Impact Assessment (DPIA);
c. Identifying data protection or security risks of existing or proposed CCTV equipment and working to address those risks with relevant colleagues and external agencies, as appropriate;
d. All data controllers and processors within BMAT handle and process CCTV footage in line with the BMAT Data Protection Policy and data protection legislation;
e. CCTV footage is obtained, stored and in line with the BMAT Data Protection Policy and data protection legislation;
f. CCTV footage is destroyed securely in line with the BMAT Data Protection Policy, the BMAT Retention Schedule and data protection legislation;
g. Informing data subjects of how their personal data will be captured by the BMAT CCTV system, of their rights in relation to the access to and destruction of CCTV footage which contains their personal data, and of the measures implemented by BMAT to protect data subjects' rights.

16. Day-to-day management of the system is the responsibility of the BMAT DPO, Operations/Facilities Managers and members of senior leadership teams ('SLT') or the BMAT Trust Executive.

IV. ACCESS TO CCTV CONTROL ROOMS AND CCTV FOOTAGE

17. All equipment or devices containing CCTV footage or images belong to BMAT as the data controller.

18. The "CCTV Request to View Form" (Appendix A) should be used to submit and authorise requests to access data obtained by the BMAT CCTV System.

19. CCTV control rooms are accessible to members of SLT, the BMAT Trust Executive, the BMAT DPO and Facilities/Operations Managers.

20. Visitors to CCTV control rooms, including other employees, may only enter if it is necessary and proportionate in pursuit of a legitimate aim and in line with the following arrangements:

a. Visits must be kept to a minimum. The BMAT DPO, Facilities/Operations Managers and members of SLT or the BMAT Trust Executive must satisfy themselves of the identity of any visitors and the purpose of their visit;
b. It is only necessary to show CCTV footage to other employees if the individual(s) recorded in the footage cannot be identified by the BMAT DPO, members of SLT or the BMAT Trust Executive or a Facilities/Operations Manager, and if the employees with whom the footage is shared are likely to be able to identify those individuals;
c. Casual visits are not permitted;
d. Visitors must be accompanied by the BMAT DPO, a Facilities/Operations Manager, a member of SLT or a member of the BMAT Trust Executive;
e. If maintenance is required, the BMAT DPO, a Facilities/Operations Manager or a member of SLT or the BMAT Trust Executive must be satisfied of the identity and purpose of contractors before allowing entry;
f. A log book is stored securely in each CCTV control room, to record the identity of visitors and the time and date of their entry and exit;
g. CCTV control rooms must be locked at all times unless the BMAT DPO, a Facilities/Operations Manager or a member of SLT or the BMAT Trust Executive is present;
h. Emergency procedures may be used in exceptional cases when the support of the emergency services is required.

21. <u>Third Party Access:</u>

a. Third party requests to access data captured by the BMAT CCTV System should be assessed by the BMAT DPO and the relevant BMAT School Principal or a suitable representative from the relevant SLT or from the BMAT Trust Executive.

b. Recordings may be viewed by the police for the prevention and detection of crime (s.29 DPA 1998) – see Appendix B to the BMAT Data Protection Policy for guidance.
c. Viewing of recordings by the police will be recorded in writing and in the log book for the relevant CCTV Control Room.
d. Footage required for evidential purposes by the police must be copied onto a separate USB drive or disc, sealed, witnessed, signed by the controller, dated and stored in a separate, secure, evidence store.
e. Recordings will only be released to the police on the clear understanding that the recording remains the property of BMAT; and that both the recording and information contained on it are to be treated in accordance with the BMAT Data Protection Policy and relevant legislation or statutory guidance;
f. If a court requires the release of an original recording, this will be produced from the secure evidence store in a sealed bag;
g. The police may ask BMAT to retain footage for possible use as evidence in the future. Such footage will be properly indexed and securely stored until needed by the police and in line with the BMAT Data Protection Policy and relevant legislation or statutory guidance,
h. Applications received from other third parties (e.g. solicitors), to view or release recordings, will be referred to the BMAT CEO and DPO, who may also refer requests to BMAT's legal advisers.

22. Access by Data Subjects.

a. Data subjects have a right to obtain confirmation that their personal data is being processed.
b. Data subjects have the right to submit a subject access request to gain access to their personal data, including data obtained by CCTV.
c. Subject access requests will be referred to the BMAT DPO and managed in line with the BMAT Data Protection Policy and relevant legislation or statutory guidance.
d. BMAT reserves the right to refuse access to CCTV footage where this would prejudice the legal rights of other individuals or jeopardise an on-going investigation.

V.STORAGE, RETENTION AND DESTRUCTION

23. Data obtained by the BMAT CCTV System is stored and retained and securely destroyed in line with the BMAT Data Protection Policy, the BMAT Retention Schedule and relevant legislation or statutory guidance. Advice should be sought from the BMAT DPO.

24. CCTV footage is stored on hard drives in each CCTV Control Room for 30 days.

25. CCTV footage must never be stored on personal USB drive and photos must never be taken of CCTV footage on personal mobile devices.

26. Password protected USBs are kept in each locked CCTV control room.

27. CCTV footage must only be transferred to the USBs by the BMAT DPO, members of SLT or the BMAT Trust Executive or a Facilities/Operations Manager, when it is necessary to store footage for longer than the time it is stored on the hard drives (e.g. because an investigation is on-going or because there is reasonable cause to believe that the footage will be needed for a future investigation);

28. CCTV files stored on the USBs must be named by date and time.

29. The transfer of CCTV footage to USB and the reason(s) for the transfer must be recorded in the log book for each CCTV Control Room and signed off by the BMAT DPO, the appropriate Facilities/Operations Manager or by a member of SLT or the BMAT Trust Executive.

30. CCTV files stored on USBs must only be accessed by the BMAT DPO, members of SLT or the BMAT Trust Executive or a Facilities/Operations Manager.

31. If footage is archived in line with the BMAT Data Protection Policy and data protection legislation or guidance, then it must be given a unique reference number (i.e. the camera location; and the date and time of the recording), logged and stored securely in the appropriate CCTV control room.

APPENDIX A: CCTV REQUEST TO VIEW FORM

Date	
Name of Person Requesting Access If the person requesting access is from an external agency, include contact details.	
Authoriser's Name (BMAT DPO, a Facilities/Operations Manager, member of SLT or member of the BMAT Trust Executive)	
Reason for request (e.g. known or suspected criminal activity). Include date and time of the incident (an approximate time window is acceptable).	

Declaration by the authoriser – I hereby authorise:

Access to the requested CCTV data by the above named person(s); and that I have clearance to authorise such access.

Signed:

Declaration by the person requesting access – I hereby understand that:

The data accessed must be used in accordance with the BMAT CCTV Policy, the BMAT Data Protection Policy and data protection legislation or guidance; and that data *remains the property of BMAT, which may refuse permission for the data to be passed onto any other individual or organisation.*

Signed: