Beacon Academy Trust

A COMPELLING VISION FOR SUCCESS

CCTV POLICY AND PROCEDURE

Approving Body	Trust
Date of First Approval	15th June, 2017
Date of Last Amendment	
To be Reviewed	Annually
Responsible Officer	BMAT MD for and on behalf of the Trust

I. INTRODUCTION

1. The purpose of this policy is to regulate the management, operation and use of the closed circuit television (CCTV) system on the premises of the Beacon Multi Academy Trust ('BMAT').

2. The system comprises a number of fixed and dome cameras located around BMAT premises. All cameras are monitored from secure central control rooms, and are only available to selected senior members of staff.

3. This policy has been drafted in compliance with:

   a. The Data Protection Act 1998 ['DPA 1998'];
   b. The Regulation of Investigatory Powers Act 2000 ['RIPA 2000'];
   c. Information Commissioner's Office Code of Conduct for CCTV; and
   d. Article 8 of the Human Rights Act 1998 ['HRA 1998'].

4. Monitoring: To keep pace with legislative changes and advances in technology, this policy is subject to annual review. Liaison meetings may be held as and when necessary with all bodies involved in the support of the BMAT CCTV system.

II. STATEMENT OF INTENT

5. BMAT is committed to ensuring the safety and wellbeing of all students, members of staff and visitors; yet respects that all individuals have a justiciable right to privacy. This policy and the procedures specified therein seek to balance these competing interests to the benefit of all concerned.

6. The objectives of this policy are as follows:

   a. To assist in managing the constituent BMAT schools and ensure the effective enforcement of key policies;
   b. To protect BMAT premises and assets;
   c. To increase personal safety and reduce the fear of crime;
   d. To support the police in a bid to deter and detect crime;
   e. To assist in identifying, apprehending and prosecuting offenders; and
   f. To protect members of the public and private property.

7. A degree of common sense runs through this policy and is expected from members of staff with clearance to access and operate the BMAT CCTV system. For obvious reasons, recording footage of children is a contentious issue; the ability to access, control and share that footage **must** be kept to a minimum.

8. The BMAT CCTV Scheme will be registered with the Information Commissioner under the terms of the DPA 1998 and will seek to comply with the requirements of the DPA 1998, the ICO Code of Practice and Article 8 of the HRA 1998.
9. BMAT will treat the system and all information, documents and recordings obtained by it as protected data in accordance with the DPA 1998.
10. Access to recorded images will be restricted to those staff authorised to view them, and will not be made more widely available.
11. Cameras will be used to monitor activities in key areas of the constituent BMAT schools, such as entranceways, corridors, car parks and other public areas to:

a. Identify criminal activity actually occurring, anticipated, or perceived; and
b. Secure the safety and well-being of students, staff and visitors.

12. Cameras are not installed in class rooms or areas where there is an increased expectation of privacy (e.g. sink areas in bathrooms).
13. Warning signs, as required by the ICO Code of Practice for CCTV use have been placed at all access routes to areas covered by the BMAT CCTV system.
14. The planning and design of the BMAT CCTV scheme has endeavoured to ensure maximum effectiveness and efficiency. However, it is not possible to guarantee that the system will cover or detect every single incident taking place in the areas of coverage.
15. Materials or knowledge secured as a result of CCTV will not be used for any commercial purpose. CCTV footage will only be released to the media for use in the investigation of a specific crime and with the written authority of the police. CCTV footage will never be released to the media for purposes of entertainment.

III. OPERATION OF THE SYSTEM

16. The BMAT CCTV scheme is administered and managed by the BMAT School Principals, in accordance with the principles and objectives stated in the ICO Code of Practice. The day-to-day management of the system is the responsibility of operations managers and members of the BMAT Senior Leadership Teams (SLT).
17. The CCTV system is operated 24 hours a day, every day of the year. Monitors are installed in CCTV control rooms, to which pictures are continuously recorded. There are CCTV control rooms at the Beal High School Upper Site, Lower Site and Sixth Form; the Forest Academy and the Beacon Business Innovation Hub.

18. The control rooms must only be staffed by SLT and operations managers. The BMAT operations managers will check and confirm the efficiency of the system daily; in particular that the equipment is properly recording and that cameras are functional.

19. Members of staff with clearance to operate the BMAT CCTV scheme have been instructed that static cameras are not to focus on private homes, gardens and other areas of private property.

20. Unless an immediate response to an event is required, CCTV cameras must not be directed or targeted at cameras at an individual, their property or a specific group of individuals, without an authorisation being obtained using the Home Office Application Form for Directed Surveillance. If granted, authorisation will last for a period of up to 3 months.

21. Members of staff with clearance to operate the BMAT CCTV system must never use it to conduct covert surveillance; only the police have the authority to conduct covert surveillance.

22. Visitors (including other members of staff) wishing to enter the CCTV control rooms should only be allowed to enter if it is necessary and proportionate in pursuit of a legitimate aim; and will be subject to particular arrangement as outlined below.

a. Visits must be kept to a minimum. The operations manager and/or member(s) of SLT must satisfy themselves over the identity of any visitors to a CCTV control room and the purpose of the visit. Where any doubt exists, access will be refused;
b. As a general rule, it is only necessary to show CCTV footage to other members of staff if the individual(s) recorded in the footage cannot be identified by members of SLT or an operations manager;
c. Casual visits will not be permitted;
d. Visitors must be accompanied by an operations manager and/or a member of SLT throughout the visit;
e. If out of hours emergency maintenance arises, the appropriate operations manager must be satisfied of the identity and purpose of contractors before allowing entry;
f. A log book will be maintained in each CCTV control room. Full details of visitors including time and date of entry and exit must be recorded;

g. CCTV control rooms must be locked at all times unless an operations manager or member of SLT is present.
h. Emergency procedures may be used in exceptional cases when the support of the emergency services is urgently required.

IV. FOOTAGE RETENTION AND SHARING PROCEDURES

23. CCTV footage is stored on hard drives in each control room for 30 days.

24. In order to maintain and preserve the integrity of the hard drives and the facility to use footage in any future proceedings, the following procedures for the use and retention of CCTV footage must be strictly adhered to:

a. CCTV footage must never be stored on personal USB drive and photos must never be taken of CCTV footage on personal mobile devices; in terms of infringement of privacy rights, this is no different to taking photos or videos of individuals on a personal mobile device without consent and taking said footage off of school premises;
b. Password protected USBs are kept in each CCTV control room. It is the responsibility of operations managers to keep the passwords and USBs secure;
c. CCTV footage must only be transferred to the USBs when it is necessary to store footage for longer than the period of time it is stored on the hard drives i.e. because an investigation is still on-going or because there is reasonable cause to believe that the footage will be needed for a future investigation;
d. CCTV footage must only be transferred to the USBs by members of SLT or an operations manager;
e. CCTV files stored on the USBs must be named by date and time.
f. The fact that footage has been transferred to a USB and the reason(s) for doing so must be recorded in the log book and signed off by the appropriate operations manager or member of SLT;
g. CCTV files stored on the USBs must only be accessed by members of SLT or an operations manager. As a general rule, it is only necessary to show CCTV footage to other members of staff if the individual(s) recorded in the footage cannot be identified by members of SLT or an operations

manager; or if the footage forms a necessary part of the evidence in formal disciplinary, capability or grievance hearings. In the minority of cases when it is necessary to show CCTV footage to other members of staff, this must be done in a CCTV control room and in strict adherence to Section IV of this policy;

h. If footage is archived then it must be given a unique reference number (i.e. camera location; and the date and time of the recording), logged and stored securely in the appropriate CCTV control room.

25. Police Access to CCTV Footage:

a. Recordings may be viewed by the police for the prevention and detection of crime (s.29 DPA 1998)

b. 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.

c. Viewing of recordings by the police must be recorded in writing and in the log book.

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 this policy.

f. BMAT also retains the right to refuse permission for the police to pass to any other person the recording or any part of the information contained thereon.

g. On occasions when a Court requires the release of an original recording, this will be produced from the secure evidence store, complete in its sealed bag.

h. The police may require 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.

26. Applications received from outside bodies (for example solicitors) to view or release recordings will be referred to the School Principal and/or BMAT's legal advisers. In these circumstances footage should only 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.

27. Access to Personal Data Captured by CCTV[1]: The DPA 1998 provides data subjects (individuals to whom 'personal data' relate) with a right to access data held about themselves, including data obtained by CCTV. 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. For further information, see the BMAT Data Protection Policy.

V. BREACH OF THIS POLICY

28. Any breach of this policy will be recorded and should be reported to the appropriate School Principal.

29. One off and/or minor breaches (e.g. asking another member of staff to identify an individual on a monitor in a CCTV control room) may just be recorded in the control room's log book.

30. Persistent and/or serious breaches (e.g. using CCTV cameras to conduct unauthorised targeted surveillance; or removing footage from the CCTV control rooms and sharing it with others) will be immediately investigated and an independent investigation will be carried out to make recommendations on how to remedy the breach.

31. Breaches may be remedied in accordance with the BMAT Disciplinary Policy.

[1] Subject to change in May 2018, following the introduction of the General Data Protection Regulation.

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 (Must be a member of SLT or an operations manager)	
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 footage 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 footage accessed must be used in accordance with the BMAT CCTV Policy and Procedure and the law contained therein; and*
- *That, if I belong to an external agency (e.g. the police), the footage remains the property of BMAT, which may refuse permission for the footage to be passed onto any other individual or organisation in writing.*

Signed: