Beacon Academy Trust

A COMPELLING VISION FOR SUCCESS

DATA PROTECTION POLICY

Approving Body	Trust
Date of Last Amendment	May 2018
To be Reviewed	May 2019 (thereafter, every three years)
Statutory (Y/N)	Y
Signed/Authorised	

I. INTRODUCTION – PURPOSE AND SCOPE

1. This policy is designed to help ensure that BMAT processes personal data in compliance with its legal obligations as a data controller, as set out in the following legislation and guidance:
    a. The Data Protection Bill 2018 ['DPA 2018'];
    b. The General Data Protection Regulation ['GDPR'];
    c. The ICO Code of Practice on the use of CCTV;
    d. The Protection of Freedoms Act 2012, in so far as we use biometric data;
    e. The ICO's ICO Code of Practice for Subject Access Requests; and
    f. Our Funding Agreement and Articles of Association.
2. More specifically, this policy shows how BMAT complies with the following principles of the GDPR, which states that personal data must be:
    a. Processed lawfully, fairly and transparently;
    b. Collected for specified, explicit and legitimate purposes;
    c. Minimised (adequate, relevant and limited to what is necessary to fulfil the purposes for processing);
    d. Accurate and kept up to date (BMAT must take reasonable steps to rectify or erase inaccurate personal data);
    e. Kept in a form which allows identification of individuals for no longer than is necessary for the purposes for which it is processed;
    f. Processed securely, to maintain its integrity and confidentiality, and ensure against unauthorised processing, accidental loss, destruction or damage;
3. Scope:
    a. This policy applies to all acts of processing personal data of a data subject by BMAT, whether in electronic or paper format.
    b. This policy applies to all BMAT employees, and to external organisations or individuals working on behalf of BMAT. Staff who fail to comply with this policy may face disciplinary action, which will consider the seriousness of the failure and the circumstances surrounding it.

II. KEY DEFINITIONS

4. 'Data' is information relating to a living person who can be identified from that data *or* from that data combined with other information in possession of the data

controller. The GDPR brings IP addresses and online identifiers (e.g. usernames) within the scope of 'data', as well as names etc.

5. 'Sensitive or special category data' on:
    a. Racial or ethnic origin;
    b. Political opinions;
    c. Religious beliefs or beliefs of a similar nature;
    d. Membership of a trade union;
    e. Physical or mental health condition;
    f. Sexual life, including sexual orientation.
6. 'Data subjects' are living individuals who are the subject of data, including job applicants, employees, students, parents or carers, governors, trustees and visitors.
7. 'Processing' covers a wide range of activities, from the collection of data to the erasure of data, including altering data, disclosing data, retrieving data, sharing data, and using data for any other purpose.
8. 'Data controller' means an individual or organisation that determines the purposes and the means of processing of personal data.
9. 'Data processor' means an individual or organisation, other than an employee of a data controller, who processes personal data on behalf of or instruction from the data controller.
10. 'Data breach' means a failure to maintain the security and integrity of personal data, leading to the destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to personal data.

III. ROLES AND RESPONSIBILITIES

11. For the purposes of this policy, BMAT is the data controller, and so is responsible for ensuring that:
    a. It is registered as such with the ICO, on an annual basis, or as otherwise required;
    b. Its constituent schools understand the requirements of this policy and the underlying legislation or guidance;
    c. Its constituent schools are meeting the requirements of this policy and the underlying legislation or guidance; and

d. That central BMAT employees (e.g. the CEO, Finance Director and HR Director) are taking steps to ensure that this policy and the underlying legislation or guidance are complied with (e.g. by managing the contracts to which BMAT is a party).

12. The BMAT CEO and Board of Trustees share responsibility for ensuring that, as data controller, BMAT fulfils its responsibilities as data controller.
13. The BMAT local governing bodies [LGB's] are responsible for monitoring and ensuring that their schools comply with their data protection obligations.
14. School principals are the representatives of the data controller for their schools; they have lead responsibility for working with the BMAT Data Protection Officer, to ensure that:
    a. Their staff understand and act in compliance with the requirements of this policy, and underlying legislation or guidance (e.g. via training);
    b. That all members of their school community, including students and parents or carers, are aware of their rights and obligations under data protection legislation (e.g. via suitable privacy notices).
15. The BMAT Data Protection Officer ['DPO'] is contactable via dpo@beaconacademytrust.co.uk. The DPO is responsible for:
    a. Monitoring compliance with this policy and underlying legislation or guidance;
    b. Informing and advising BMAT on its legal obligations, including the BMAT CEO, BMAT trustees and LGBs, and BMAT school principals;
    c. Advising on impact assessments when new data processing activities are proposed or introduced;
    d. Being the first point of contact for data subjects and the ICO;
    e. Assigning responsibilities and conducting audits;
    f. Raising awareness and training staff;
    g. Developing related policies and guidelines where applicable; and
    h. Providing an annual report of their activities to the Board of Trustees and, where relevant, reporting their recommendations on data protection issues to the CEO and/or Board of Trustees.
16. BMAT employees with leadership roles (e.g. heads of department, directors of achievement and progress, and members of SLT) are responsible for:

a. Ensuring that their teams are cognisant of and act in compliance with this policy, and the underlying legislation or guidance;
b. Monitoring data security within their teams, and acting to prevent non-compliance. This includes keeping a record of the removal of personal data from BMAT premises, e.g. for department assessments (Section XII contains more information on taking personal data off-site).

17. All BMAT employees are responsible for:
    a. Collecting, storing and processing any personal data in accordance with this policy;
    b. Informing BMAT of any changes to their personal data, such as a change of address, by notifying data@beaconacademytrust.co.uk and hr@beaconacademytrust.co.uk.
    c. Contacting the DPO in the following circumstances:
        i. With any questions about the operation of this policy or underlying legislation and guidance;
        ii. With any concerns that this policy is not being followed, however minor;
        iii. If they are unsure if they have a lawful basis for collecting or processing personal data and/or if they need to rely on consent;
        iv. If they need to draft a privacy notice or deal with data protection rights invoked by an individual (e.g. a subject access request);
        v. If there has been a data breach, however minor, and in whatever form (e.g. student information lost or left in public, or unauthorised access to information held on a computer);
        vi. Whenever they propose a new activity that may affect the privacy rights of individuals (e.g. a school play that will involve sending details of the cast to the public and/or press, including photos);
        vii. If they need help with contracts or sharing personal data with third parties, including law enforcement or government agents.

IV. COLLECTING PERSONAL DATA.

18. *Lawfulness, fairness and transparency* - BMAT will only collect personal data when it has one of the following six lawful bases for doing so:

a. The data is necessary for BMAT to fulfil a contract with the data subject (e.g. a contract of employment, or where the data subject has asked BMAT to take specific steps before entering into a contract).
b. The data needs to be processed so that BMAT and/or a constituent BMAT school can comply with a legal obligation (e.g. contact details for parents/carers are necessary for BMAT to comply with its legal obligation to safeguard its students).
c. The data needs to be processed to ensure the vital interests of the individual i.e. to protect someone's life.
d. The data needs to be processed so that BMAT, as a public authority, can perform a task in the public interest, and carry out its official functions (e.g. produce aggregated data reports under the Public-Sector Equality Duty).
e. The data needs to be processed for the legitimate interests of BMAT or a third party, only insofar as the rights and freedoms of the data subject(s) are not overridden (e.g. to ensure the efficient operation of school administration, IT and security systems).
f. The individual (or their parent/carer when appropriate in the case of a pupil) has given free, informed and explicit consent. Where possible and lawful, the need for consent will be avoided. However, consent will be required e.g. if BMAT requests to share personal data for marketing, press or other publicity purposes.

19. If BMAT offers online services to students, such as classroom based apps, and intends to rely on consent as a basis for processing, it will get parental consent where the pupil is under 13 (with the exception of online counselling and preventative services).
20. *Lawfulness, fairness and transparency* - for special categories of personal data, BMAT will also meet one of the special category conditions for processing, i.e. processing is necessary:
    a. To fulfil employment law obligations;
    b. To protect individuals' vital interests (e.g. passing on health information when an individual is unconscious).
    c. To establish, exercise or defend a legal claim (i.e. whenever courts are acting in their judicial capacity).

d. For substantial public interest, on a legal basis (e.g. BMAT has a legal duty to protect the safety of its students and employees, so it processes data on health conditions. The Public-Sector Equality Duty also requires BMAT to process data on e.g. ethnicity). If BMAT processes special category data for reasons of substantial public interest, it will ensure that the processing is proportionate to the aim pursued, respects the essence of the right to data protection, and provides for suitable and specific measures to safeguard the fundamental rights and the interests of data subject(s).
e. For Reasons of public interest, in areas of public health.
f. For archiving purposes in the public interest (or scientific or historical research purposes or statistical purposes).

21. *Limitation, minimisation and accuracy* – BMAT will only collect personal data for specified, explicit and legitimate reasons. This will help to ensure that BMAT only collects and processes a proportionate amount of data. BMAT will:
    a. Clearly explain the specific reasons for collecting personal data and relevant information required by data protection law., to individual data subjects, when we first collect their data (in almost all cases, this will be in the form of privacy notices);
    b. Contact data subjects again if BMAT seeks or needs to use their personal data for reasons other than those given when it was first collected, and seek their consent if necessary;
    c. Only process personal data when it is necessary for BMAT, an employee or a department to perform their role(s);
    d. Ensure that personal data is deleted and anonymised or aggregated when it is no longer needed for the specified and communicated reasons, in accordance with Appendix A - the BMAT Data Retention Schedule.

V. SHARING PERSONAL DATA1

22. BMAT will not normally share personal data with third parties. However, BMAT may share personal data if:
    a. A student or parent/carer puts the safety of BMAT employee(s) at risk;
    b. BMAT needs to liaise with other agencies, such as social services or a local authority. We will seek consent before doing so, if necessary;

c. The suppliers or contractors used by BMAT need data to provide services to BMAT employees, students and parents/carers (for example, software companies). When doing this, BMAT will:
    i. Only appoint suppliers or contractors that provide sufficient guarantees that they comply with data protection legislation;
    ii. Establish a data sharing agreement with each supplier or contractor, to ensure the fair and lawful processing of shared personal data. This will usually be in the terms of contract, but may be in a standalone agreement.
    iii. Minimise the amount of data we share by only sharing it to the extent that it is necessary for the supplier or contractor to carry out their service.

23. BMAT may also share personal data when it is legally required to do so, e.g. by law enforcement and government bodies. For example, when personal data is needed:
    a. To enable BMAT to fulfil its safeguarding obligations;
    b. To enable emergency services and local authorities to respond to an emergency or crisis involving BMAT students or employees;
    c. To help prevent or detect crime;
    d. To apprehend or prosecute offenders;
    e. In connection to legal proceedings;
    f. To enable HMRC to assess or collect tax owed to them;
    g. For research and statistical purposes, if the data is anonymised/aggregated, or informed consent has been obtained.
24. In some cases, BMAT will have a discretion, rather than a duty, to share personal data with law enforcement agencies; and in some cases, informed consent should be obtained. For more guidance, see Appendix B - Sharing Data with Law Enforcement Agencies.
25. If BMAT ever transfers personal data outside the EEA, it will do so in accordance with data protection legislation and guidance.

VI. THE RIGHTS OF DATA SUBJECTS: SUBJECT ACCESS REQUESTS

26. Data subjects are entitled to submit subject access requests to BMAT, to access personal data that it holds as a data controller. Data subjects are only entitled to

make subject access requests concerning the processing of their own personal data.

27. Data subjects may request:
    a. Confirmation that their personal data is being processed;
    b. Access to a copy of the personal data that is held on them;
    c. Confirmation of the purpose(s) for processing their personal data;
    d. Details on whether their personal data has been or will be shared with any third party;
    e. How long their data will be retained for, or the criteria that will be used to determine how long their data will be retained for, if it is not possible to specify an exact period;
    f. How their data was collected, if it did not come from the data subject;
    g. Whether their data is subject to any automated decision making, including the potential consequences.
28. Subject access requests must be submitted in writing to the BMAT DPO, at dpo@beaconacademytrust.co.uk or 'Data Protection Officer, The Beacon Multi-Academy Trust, Woodford Bridge Road, Ilford, IG4 5LP. Requests must include:
    a. The name and contact details of the data subject; and
    b. Details of the information requested.
29. BMAT employees who receive a subject access request must not respond to it and must forward it to the BMAT DPO immediately.
30. Student Subject Access Requests:
    a. The law presumes that children aged 12 or above have sufficient maturity to understand their data rights and make their own subject access requests.
    b. As a result, subject access requests from parents or carers, made on behalf of a BMAT student, will not normally be granted without informed and explicit consent from that student.
    c. However, a student's ability to understand their data rights will be considered; if a student aged 12 or above does not have sufficient maturity and/or ability to understand their data rights, then subject access requests from parents or carers made on behalf of that student may be granted.
31. Parental requests to access a student's educational record:

a. There is no automatic parental right to access the educational record of a student at academies and free schools.
b. BMAT will consider such requests if they are made in writing to the BMAT DPO, at dpo@beaconacademytrust.co.uk or 'Data Protection Officer, The Beacon Multi-Academy Trust, Woodford Bridge Road, Ilford, IG4 5LP.
c. Following such a request, the DPO will liaise with the appropriate school principal to determine if the request should be granted.
d. BMAT may seek consent from the student in question, particularly if the student is in Year 9 or above, and if there is reason to believe that the student's relationship with his/her parents or carers is fragile.
e. If BMAT grants a parental request to access a student's educational record, it will do so within one month of receipt.

32. When responding to subject access requests, BMAT:
    a. May ask the alleged data subject to provide two forms of identification;
    b. May contact the alleged data subject to confirm that the request is genuine;
    c. Will endeavour to respond within one month of receiving the request;
    d. May inform the data subject in writing and within one month of receiving their request, that it will be complied with within three months of receipt, because it is complex and/or because the request contains multiple sub-requests.
33. Following a subject access request, BMAT will not disclose personal data if doing so:
    a. May cause harm to the physical or mental health of a BMAT student, employee or other identified individual;
    b. Would reveal that a child is at risk of abuse, if doing so would not serve that child's best interests;
    c. Would disclose information contained in adoption or parental order records;
    d. Would disclose information that is given to a court in proceedings concerning a child that is subject to or involved in the request.
34. Excessive and/or unfounded subject access requests:
    a. BMAT may refuse to act on unfounded and/or excessive subject access requests;

b. If BMAT acts on an unfounded and/or excessive subject access request, it may charge a reasonable fee for doing so, taking administrative costs into account;
c. Repetitive requests, and requests that ask for multiple copies of the same information, will be determined as unfounded and excessive;
d. If BMAT has reasonable grounds to believe that an individual is submitting excessive and/or unfounded subject access requests, to waste time and/or to be vexatious or malicious, it will consider taking legal action, and will seek to recover the cost of doing so from the individual in question.

35. If BMAT refuses a subject access request, it will inform the individual why in writing, and inform them that they have the right to complain to the ICO.

VII. OTHER RIGHTS OF DATA SUBJECTS

36. The most exercised right of data subjects is the right to submit a subject access request, as above. However, data subjects also have the right to:
    a. Withdraw their consent to processing their personal data, at any time, if consent was the basis for processing the data;
    b. Requesting the rectification, erasure or restricted processing of their personal data;
    c. Prevent their personal data being used for direct marketing;
    d. Complain to the ICO;
    e. Be notified of a data breach in certain circumstances (Section XIII, below);
    f. Request that their personal data be transferred to a third party, in certain circumstances;
    g. Challenge the processing of personal data based on public interest;
    h. Challenge decisions concerning their personal data based solely on automated decision making, that might negatively affect them;
    i. Prevent processing that is likely to cause material damage or distress;
    j. Request a copy of agreements for transferring their personal data outside of the EEA;
37. To exercise any of these rights, data subjects must submit a written request to the BMAT DPO, at dpo@beaconacademytrust.co.uk or ‘Data Protection Officer, The Beacon Multi-Academy Trust, Ilford, IG4 5LP. BMAT employees who receive

such a request must not respond to it and must forward it to the BMAT DPO immediately.

VIII. BIOMETRIC DATA RECOGNITION SYSTEMS

38. BMAT uses student and employee fingerprint data, as part of 'Parent Pay' - an automated biometric recognition system, which enables us to operate a cashless system, in the interests of efficiency and safety on BMAT premises. BMAT's use of biometric data complies with the Protection of Freedoms Act 2012:

39. BMAT Students:

    a. Parents/carers are notified before their child first takes part in the Parent Pay biometric recognition system;
    b. Written consent is obtained from at least one parent/carer before we take and process biometric data from a student;
    c. Parents/carers and students may choose not to provide their biometric data for Parent Pay. When this right is exercised, BMAT will make arrangements for the student in question to access the relevant services. For example, parents/carers can pay for school dinners up front by cheque or transfer;
    d. Parents/carers and students can withdraw consent to participate in Parent Pay at any time, by submitting a written request to the BMAT DPO, at dpo@beaconacademytrust.co.uk or 'Data Protection Officer, The Beacon Multi-Academy Trust, Ilford, IG4 5LP. BMAT employees who receive such a request must not respond to it and must forward it to the BMAT DPO immediately;
    e. As required by law, if a student refuses to participate, or continue to participate, in Parent Pay, their biometric data will not be processed, irrespective of parental consent;
    f. If consent is withdrawn, any biometric data already captured will be deleted.

40. BMAT employees: Consent will also be obtained from employees before processing their biometric data for Parent Pay. The above provisions, on the right to refuse or withdraw consent and be provided with alternative means of payment, apply.

IX. CCTV, PHOTOGRAPHS AND VIDEOS

41. BMAT uses CCTV to ensure that its premises remain safe and secure for students, employees and the wider community; CCTV helps BMAT to comply with its obligation to safeguard students. BMAT complies with the ICO Code of Practice on the use of CCTV, and its CCTV scheme is registered with the ICO.
    a. Consent is not required to use CCTV, but BMAT makes it clear when and where individuals are being recorded. Cameras are prominently signposted and clearly visible.
    b. More information on the BMAT CCTV system is contained in the BMAT CCTV Policy.
    c. Queries should be directed to the BMAT DPO, at dpo@beaconacademytrust.co.uk or 'Data Protection Officer, The Beacon Multi-Academy Trust, Ilford, IG4 5LP. BMAT employees who receive such a request must not respond to it and must forward it to the BMAT DPO immediately.
42. As part of school activities (e.g. trips and plays), BMAT may take photographs and record images of individuals:
    a. Written consent will be obtained from parents/carers, or from students aged 18 or over, for photographs or videos to be used for marketing, promotional or other communication purposes (e.g. in newsletters, on school notice boards, by external agencies such as newspapers, and online on a school website or social media page).
    b. If consent is required, BMAT will clearly explain what purposes the photographs or videos will be used for, to parents/carers *and* students.
    c. Consent may be refused or withdrawn at any time. If consent is withdrawn, BMAT will delete the photograph or video and will not distribute it further;
    d. Employees who need to obtain consent to take photos and/or record images of students should contact the BMAT DPO, who will have a template privacy notice and/or be able to assist with the drafting of an appropriate privacy notice (Section XI contains more information on privacy notices).

XI. EFFECTIVE COMPLIANCE: PRIVACY NOTICES, IMPACT ASSESSMENTS, AUDITS AND REVIEWS

43. Privacy Notices: BMAT will communicate how it uses and processes the personal data of data subjects via privacy notices. The BMAT DPO is responsible for overseeing privacy notices; s/he should be consulted whenever a new privacy notice needs to be drafted. BMAT privacy notices will:
    a. Be concise, transparent, easily accessible, free of charge, written in plain language and adapted to child data subjects so that the contents can be fully understood (e.g. “your information will be kept for…” rather than “the retention period for your data is…”).
    b. Be provided to data subjects when their data is collected for the first time (e.g. when a student enrols with BMAT or a new employee joins BMAT);
    c. Identify BMAT as the data controller, and provide contact details of the BMAT DPO;
    d. Explain the purpose(s), legal basis or legitimate interests of the data controller for the processing, including whether there is a statutory or contractual obligation to process the data;
    e. List any recipients of the data, including any safeguards, particularly if the data is transferred outside of the EEA;
    f. Where possible, list the period for which the data will be stored, or the criteria for determining for how long it will be stored;
    g. Explain the data subject’s right to withdraw consent, and to lodge a complaint with the ICO;
    h. Explain the consequences of failing to provide data, including whether the data is required to enter into a contract; and
    i. Whether the data will be subject to automated-decision making.
44. Impact assessments: Under the supervision of the DPO, BMAT will perform impact assessments when it proposes to implement a new data processing system, which is likely to result in a high-risk to the rights and freedoms of individuals. Impact assessments will be tailored to the proposed system; broadly speaking, they should map out the process that individual data subjects and their data will go through, if the new system is implemented. Any risks should be identified, and balanced against the justification for the proposed system. Factors that may indicate a high risk include, but are not limited to:
    a. Data processing on a large scale;
    b. Data concerning vulnerable data subjects;

c. A system involving the processing of special category data;
d. A system involving automatic-decision making and/or systematic monitoring;
e. A system involving the transfer of data outside of the EEA.

45. In addition to publishing and reviewing this policy, as above, to ensure ongoing compliance, BMAT will
    a. Regularly train its employees on this policy and matters of data protection law, including induction training for all new employees, governors and trustees;
    b. Conduct regular audits and reviews of connected policies and data processing systems;
    c. For all personal data held, maintain an internal record of the type of data, data subject, purpose of processing, extent of sharing, retention periods and security measure.

XII. DATA SECURITY, STORAGE AND DISPOSAL

46. BMAT will protect personal data against accidental or unlawful loss, destruction or damage; and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure:
    a. All BMAT employees should ensure that paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data, are stored under lock and key when not in use. This includes personal data stored in classrooms, department offices, staff rooms and at home;
    b. All BMAT employees should think carefully before taking personal data off-site, and extracting or printing personal data from a secure system (e.g. SIMs). In most cases, extraction is not necessary, and an individual preference for paper records is not sufficient to override the risk of storing personal data in a non-secure format;
    c. Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access;
    d. Personal data should only be taken off-site when necessary; taking personal data off-site should generally be avoided. Department leads are

responsible for monitoring the removal of personal data from BMAT premises within their department. This includes removing student exercise books and mark-sheets for department assessments and/or evaluation. Department leads should keep a record of the data being taken off site, by whom and for what time period. Department leads should also instruct their teams to store data securely when off-site.

g. Before sharing personal data with a third party, reasonable steps are taken to ensure it is stored securely and adequately protected (see Section V – Sharing Personal Data).

47. Secure disposal of personal data: Personal data that is no longer needed will be disposed of securely. Inaccurate personal data will be rectified or disposed of securely. For example:
    a. Outdated or inaccurate paper-based records will be shredded;
    b. Electronic files will be overwritten or deleted;
    c. Where third parties are used to safely dispose of records, BMAT will require the third party to provide sufficient guarantees that it will comply data protection law in doing so (Section V – Sharing Personal Data).

XIII. PERSONAL DATA BREACHES

48. BMAT and its employees will take all reasonable steps to ensure that no personal data breaches occur. In the event of a suspected data breach, the following procedure will be followed, which is based on ICO Guidance on Personal Data Breaches.
49. On discovering or causing a breach or potential breach, the employee or data processor must immediately notify the BMAT DPO, outlining:
    a. The data that is or is believed to be affected;
    b. The person(s) responsible or involved;
    c. Any other points that will assist the DPO in investigating the breach or potential breach.
50. The BMAT DPO will investigate the report, and determine whether a breach has occurred. A breach will have occurred if personal data has accidentally or unlawfully been:
    a. Lost (e.g. a record of student information was misplaced by a teacher);
    b. Stolen (e.g. a work laptop);

c. Destroyed (e.g. accidental deletion of an electronic file, or disposal of a paper file);
d. Altered (e.g. alteration of an electronic record on a data subject);
e. Disclosed or made available where it should not have been (e.g. sharing personal data with a third party without consent, if consent was required);
f. Made available to unauthorised persons (e.g. shared with third parties other than those with whom it was necessary or permitted to share with).

42. If a breach has occurred, the DPO will alert the appropriate school principal, and the BMAT CEO where appropriate. If the breach is minor, a simple report will suffice. If the breach is serious, the DPO will work with the appropriate school principal and/or the BMAT CEO to mitigate the impact on data subject(s).
43. The DPO will record all breaches on behalf of BMAT, and store them securely, even if they do not result in disclosure to the ICO (because a decision not to disclose to the ICO may be challenged at a later date). For each breach, this record will include the:
    a. Facts, cause and impact; and
    b. Action(s) taken to counter and contain the breach, and ensure that it does not repeat.
44. The DPO will take all reasonable steps to contain and minimise the impact of the breach, assisted by relevant employees and/or data processors if necessary.
45. The DPO will determine whether the breach must be reported to the ICO:
    a. The test for reporting is whether the breach is likely to result in a risk to the rights and freedoms of individuals, and cause them any damage, which includes emotional distress.
    b. 'Damage' could include or result from the loss of data, identity theft or fraud, monetary loss, the reversal of pseudonymisation, reputational damage, the disclosure of sensitive information (e.g. health conditions or disciplinary records), and loss of confidentiality.
    c. Breaches which meet the above test must be reported to the ICO within 72 hours of the breach being discovered, via the Report a Breach section of the ICO website.

d. Reports to the ICO must include a description of the nature of the breach including the contact details of the DPO and, where known:
    i. The categories and approximate number of individuals concerned;
    ii. The categories and approximate number of personal data records concerned;
    iii. A description of the likely consequences of the breach; and
    iv. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse impact on those affected.
e. If any of the above details are not known, the DPO will explain why there is a delay and when s/he expects to have the information, which s/he will report as soon as possible.

46. The DPO will determine whether the affected individuals also need to be informed of the breach. This will be necessary if the risk of an impact to the rights and freedoms of those individuals is high. If it is, the DPO will inform them of the breach, in writing, specifying:
    a. Their name and contact details;
    b. A description of the likely consequences of the personal data breach;
    c. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any adverse impact on the individual(s) concerned.
47. If a breach is reported to the ICO and/or individuals, the DPO will meet promptly with the BMAT CEO and/or the appropriate school principal, to review the breach and decide and how to avoid a repeat.
48. <u>Actions to mitigate the impact of specific and particularly sensitive forms of data breach:</u>
    a. <u>The disclosure of sensitive information (e.g. safeguarding records) via email:</u>
        i. The sender must attempt to recall the email as soon as they become aware of the breach;
        ii. Employees who receive the email must alert the sender and the DPO immediately;

iii. The DPO will determine if the ICO and the affected individuals need to be contacted, as above;
iv. If the sender is unavailable, the DPO will ask a member of IT staff to attempt to recall the email;
v. If recall is unsuccessful, the DPO will contact any unauthorised individuals with whom the data has been shared, explain that it was sent in error, and instruct that the information is deleted and not shared, published, saved or copied;
vi. The DPO will ensure that a written response is received from all the individuals who received the data, confirming that they have complied with this instruction;
vii. The DPO will carry out checks to ensure that the information has not been made public; if it has, s/he will contact the relevant publisher or website owner, to request that the information is removed and deleted.

b. <u>A BMAT laptop containing non-encrypted sensitive personal data being stolen or hacked:</u>
   i. The member of staff from whom the laptop was stolen must report the theft to the police and the BMAT DPO, immediately;
   ii. The member of staff from whom the laptop was stolen must attempt to list the personal data stored on the laptop, and the individuals affected;
   iii. The DPO will determine if the ICO and affected individuals need to be contacted, as above;
   iv. If the data concerned was stored on software (e.g. SIMs), the DPO will work with the relevant data processor and internal IT staff, to determine if that access to that software can be blocked remotely.
   v. The DPO will carry out checks to ensure that the information has not been made public; if it has, s/he will contact the relevant publisher or website owner, to request that the information is removed and deleted.

c. <u>Parent Pay being hacked and parents' financial details stolen:</u>

i. If the DPO did not discover the breach, s/he must be informed immediately;
ii. The DPO will attempt to determine the source of the breach and work with the relevant data processor to prevent any further theft of data;
iii. The DPO will report the incident to the police;
iv. The DPO and relevant data processor will determine the number of affected individuals;
v. The DPO will report the breach to the ICO, and the affected individuals will be informed;
vi. On behalf of BMAT, the DPO will work with relevant third parties (e.g. banks) to mitigate the impact of the breach.

APPENDIX A – BMAT DATA RETENTION SCHEDULE

MANAGEMENT OF BMAT SCHOOLS: BOARD OF TRUSTEES AND LGBs				
Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period
Articles of association and funding agreement	No		Permanent	
Action plans	No		Life of plan +3 years	Secure disposal
Policy documents	No		Life of policy +3 years	
Records of complaints	Yes		Date of resolution +6 years and more in case of contentious disputes	Secure disposal
Minutes of meetings	Yes			Secure disposal
Reports to Trustees or LGBs	Yes			Secure disposal
MANAGEMENT OF BMAT SCHOOLS: THE TRUST EXECUTIVE AND SLT				
School development plans	No			
Minutes of meetings	Yes			Secure disposal
MANAGEMENT OF BMAT SCHOOLS: ADMISSIONS PROCESS				
Successful admissions	Yes	School Admissions Code 2014	Date of admission +1 year	Secure disposal
Unsuccessful admissions	Yes	School Admissions Code 2014	Resolution of case +1 year	Secure disposal
Register of admissions	Yes	School Attendance: Departmental Advice 2014	3 years for each entry after date on which entry was made	Secure disposal
Proof of address	Yes	School Admissions Code 2014	Current year +1 year	Secure disposal

Supplementary information (e.g. religion, medical conditions)	Yes		Added to student file for successful admissions. Deleted after appeal process expires for unsuccessful admissions.	Secure disposal
Admissions policies	No	School Admissions Code 2014	Life of policy +3 years	Secure disposal
MANAGEMENT OF BMAT SCHOOLS: OPERATIONAL ADMINISTRATION				
Visitors' books/signing in sheets	Yes		Current year +6 years	Secure disposal
HUMAN RESOURCES: RECRUITMENT				
Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period
Records leading to appointment of new school principal	Yes		Date of appointment +6 years	Secure disposal
Records leading to appointment of new employee	Yes		Date of appointment +6 months (relevant info added to personnel file for successful candidates)	Secure disposal
DBS checks	Yes	Keeping Children Safe in Education 2016	Schools do not have to keep copies of DBS certificates and must not do so for more than 6 months	Secure disposal
Proof of identity and right to work checks	Yes		Added to personnel file (see below)	

HUMAN RESOURCES: OPERATIONAL STAFF MANAGEMENT				
Personnel file	Yes	Limitation Act 1980	Termination of employment +6 years	Secure disposal
Appraisal records	Yes		Current year +5 years	Secure disposal
HUMAN RESOURCES: DISCIPLINARY AND GRIEVANCE PROCEDURES				
Disciplinary proceedings	Yes			Secure disposal (records to be removed from personnel files, if added)
Allegations of child protection nature	Yes	Keeping Children Safe in Education 2016	Individual's normal retirement age or 10 years from date of allegation, whichever is longer	Secure disposal (must be shredded)
HUMAN RESOURCES: PAYROLL AND PENSIONS				
Maternity pay records	Yes	Statutory Maternity Pay Regulations 1986	Current year +3 years	Secure disposal
Records held under Retirement Benefits Schemes	Yes	Information Powers Regulations 1995	Current year +6 years	Secure disposal
HUMAN RESOURCES: HEALTH AND SAFETY				
H&S Policy Statements	No		Life of policy +3 years	Secure disposal
Risk assessments	No		Life of assessment +3years	Secure disposal
Records re: injury at work	Yes		Date of incident +12 years	Secure disposal

Accident reports	Yes	Social Security (Claims and Payments) Regulations 1979 Regulation 25. Social Security Administration Act 1992 Section 8. Limitation Act 1980	Date of incident +6 years (adults); +12 years (child)	Secure disposal
Fire precautions log books	No		Current year +6 years	Secure disposal
COSHH	No	Control of Substances Hazardous to Health Regulations 2002. SI 2002 No 2677 Regulation 11; Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Current year +40 years	Secure disposal
Asbestos records	No	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action +40 years	Secure disposal
FINANCIAL MANAGEMENT: RISK MANAGEMENT AND INSURANCE				
Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period
Employer's Liability Insurance Certificate				Secure disposal

FINANCIAL MANAGEMENT: ASSET MANAGEMENT				
Inventories				
Burglary/theft/vandalism reports				
FINANCIAL MANAGEMENT: ACCOUNTS AND BUDGET MANAGEMENT				
Annual Accounts				
Records: re creation and management of budgets				
Invoices, receipts, order books, requisitions, delivery notices				
Records re: debt collection				
PREMISES MANAGEMENT				
Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period
Title deeds of properties belonging to BMAT	No		Permanent	
Plans of BMAT property	No		As long as property belongs to BMAT	Passed onto new owners, if applicable
Records re: letting of BMAT premises	No		Current financial year + 6 years	Secure disposal
Records re: maintenance of premises	No		Current year +6 years	Secure disposal
STUDENT MANAGEMENT: EDUCATIONAL RECORD				
Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period

Student's educational record	Yes	Education (Pupil Information) (England) Regulations 2005; Limitation Act 1980	DoB of student +25 years	Secure disposal
Child protection info held on student file	Yes	Keeping Children Safe in Education 2016	Same as student file	Secure disposal (must be shredded)
Child protection info held in separate file(s)	Yes	Keeping Children Safe in Education 2016	DoB of student +25 years	Secure disposal (must be shredded)
STUDENT MANAGEMENT: ATTENDANCE				
Attendance Registers	Yes	School attendance: Departmental advice for maintained schools, academies, independent schools and local authorities October 2014	3 years after date on which each entry on register was made	Secure disposal
Records of authorised absences	Yes	Education Act 1996, Section 7	Current academic year + 2 years	Secure disposal
Records of medical rooms	Yes			
STUDENT MANAGEMENT: SEND				
Files, reviews and education plans	Yes	Limitation Act 1980	DoB of student + 25 years	Secure disposal
Statement maintained under Section 234 Education Act 1990	Yes	Education Act 1996; SEND Act 2001, Section 1	DoB of student + 25 years	Secure disposal
Accessibility Strategy	Yes	Education Act 1996; SEND Act 2001, Section 14	DoB of student + 25 years	Secure disposal
CURRICULUM MANAGEMENT: STATISTICS AND MANAGEMENT INFORMATION				

Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period
Exam results	Yes		Current year +6 years	Secure disposal
Exam papers	Yes		Until any appeals/validation process is complete	Secure disposal
PAN reports	Yes		Current year +6 years	Secure disposal
Value added/contextual data	Yes		Current year +6 years	Secure disposal
CURRICULUM MANAGEMENT: IMPLEMENTATION				
Schemes of work	No			Secure disposal
Students' work	Yes			Secure disposal
Mark books	Yes (unless anonymised)			Secure disposal
Record of homework set	No			Secure disposal
Timetable	No			Secure disposal
EXTRA-CURRICULAR ACTIVITIES				
Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period
Consent forms for trips with no major incident	Yes		End of the trip	Secure disposal
Consent forms for trips with major incident	Yes	Limitation Act 1980	DOB of the student(s) involved in incident +25 years.	Secure disposal
Records re: approval to run an external trip	No	Outdoor Education Advisers' Panel National Guidance	Date of visit + 10 years	Secure disposal
CENTRAL GOVERNMENT & LOCAL AUTHORITY				
Description	Data prot. issues	Statutory provisions	Retention Period	Actions at end of period
OFSTED reports	No		Life of the report, then review	Secure disposal
Census reports	No		Current year +5 years	Secure disposal

Attendance returns	Yes		Current year +1 year	Secure disposal

APPENDIX B – SHARING DATA WITH LAW ENFORCEMENT AGENCIES

- Personal data belongs to the data subject, so their informed consent is normally required before sharing it with third parties, including the police; BMAT employees should not assume that they are obliged to comply with a data access request from the police, and should bear the seniority of the requesting officers in mind.

- If informed consent from the data subject is not obtained, then personal data may only be shared if there is a duty or power in law to share the requested information.

- If there is a duty, then disclosure is mandatory and consent is not necessary. This is rare and unlikely to apply in the school context. The main examples are:
    - A court order, which must be served on the school (unless the school decides to challenge the order in court);
    - A duty to inform the police of information about terrorist activity (Prevention of Terrorism Act 1989 and Terrorism Act 2000).

- If there is a legal power, then BMAT may disclose, but must consider the implications of gaining consent. The main examples are:
    - BMAT may pass on information to the Police if it believes that someone may be seriously harmed (Police and Criminal Evidence Act 1984). This will apply in very limited circumstances.
    - Information may be required on an individual for strategic cross organisational planning to detect, prevent or reduce crime and disorder that an individual may be involved in (Crime and Disorder Act 1998). A designated officer would deal with and make these requests, not a CPO or PO. BMAT would be expected to consider the strength of evidence that an individual is involved, the likelihood that sharing the information will detect, prevent or reduce crime, the proportionality of the request and the likely effectiveness of the claimed strategy.
    - A Section 29(3) Exemption (where consent may be prejudicial to an investigation to the prevention and detection of crime or the apprehension or prosecution of offenders). A Section 29(3) form, signed by an Inspector, would need to be served on BMAT. BMAT does not have to share the information, and should ask why/what is needed before making a decision (e.g. does the form demonstrate a clear risk that the individual may destroy evidence or abscond?)
    - A different power exists where BMAT chooses to share information on an individual without a preceding police request: if a school suspects a child is being abused, it has a legal power to disclose information to Social Services and/or the police. As above, schools must consider whether gaining consent or informing the child/parents would be beneficial or detrimental. If the latter, then disclosure without consent is allowed.