The Boston Witham Academies Federation

Data Protection Policy

Monitoring Responsibility	COO
Next Review Date	September 2021
Approval Body	People
Date Ratified	September 14th 2020
Chair of Committee Signature	

Contents

1. Introduction

This document sets out The Boston Witham Academies Federation's (the Trust) and its Academies' responsibilities under the General Data Protection Regulation (GDPR) 2018 (the Regulation) and provides guidance on the maintenance of and access to data, including employment and educational records in accordance with the provisions of the Regulation.

1.1 The General Data Protection Regulation

The GDPR (Regulation (EU) 2016/679) is a binding, legislative regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The Regulation came into force on 25 May 2018 and replaces the Data Protection Act 1998, with many of the main concepts and principles remaining the same but with new elements and significant enhancements added.

The Regulation provides that:

- anyone who records and uses personal information (data controllers/users) must be open about how the information is used and must follow the six principles of 'good information handling'.
- all individuals (data subjects) have the right to see information that is held about them and the right to rectification if incorrect.
- The Regulation applies to all electronic records that contain information about living and identifiable individuals and extends data protection to manual files where the personal data of a data subject is readily accessible (a structured filing system).
- The main aim of the Regulation is to protect data from unnecessary, unauthorised or harmful use and to provide individuals with some control over the use of their personal data. Individuals have the right to take action for compensation caused by inaccurate, lost or destroyed data or unauthorised disclosure of information. They also have the right to complain to the Information Commissioner who may serve an enforcement notice and, in some circumstances, impose a financial penalty.

1.2 Notification

The Boston Witham Academies Federation is registered with the Information Commissioner's Office (ICO) as data controller for all Trust and Academy data. The Chief Operating Officer, as Data Protection Officer is responsible for maintaining the record with the ICO.

Each Head of Academy and Trust Manager must advise the Data Protection Officer if there are any changes to the use of personal data that are not covered by the Trust registration.

2. Principles of Data Protection

In collecting, using, storing and disposing of data, the Trust or Academy will comply with the requirements of the Regulation that govern the processing of personal data. Under these requirements, the information will be collected and used fairly, stored safely and not disclosed to any other person where to do so would be in breach of those requirements or would otherwise be unlawful.

The Trust will maintain documentation of the key data it holds, the systems for processing that data and the consents that are required to enable the processing.

All Trust staff who process or use personal information will ensure they comply with the following seven data protection principles which are laid out in the GDPR Regulation.

Article 5 of the Regulation requires that personal data shall be:

- **Principle 1** - Processed fairly, lawfully and in a transparent manner in relation to the data subject
- **Principle 2 -** Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- **Principle 3 -** Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- **Principle 4 -** accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Principle 5 -** Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.
- **Principle 6 -** Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Principle 7 –** The Data Controller shall be responsible for, and be able to demonstrate compliance with the GDPR data processing principles.

3. Transfer of Information Outside the European Economic Area (EEA)

Personal data shall not be transferred outside of the EEA unless that country or territory ensures an adequate level of protection. Certain countries/territories have been certified as providing an adequate level of protection. Where it is proposed to transfer to a country/territory that has not been certified, the Data Controller must satisfy itself that the country/territory affords an adequate level of protection.

If the data is to be transferred to a country or territory that does not have adequate protection, then the Chief Operating Officer must approve the transfer and this approval will only be granted if it can be demonstrated that there is a legal basis for the processing.

4. Individuals' Rights

The GDPR provides the following rights for individuals:

4.1 The Right to be Informed

This right encompasses the Trust's obligation to provide 'fair processing information', typically through a privacy notice. Each Academy will publish a Privacy Notice on their website and have a copy available at the Academy reception.

4.2 The Right of Access

Under the GDPR, individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information (largely provided in a privacy notice).

Subject Access Requests are covered in Annex C of this policy and all such requests should be directed to the Trust's Data Protection Officer.

4.3 The Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete and to block future processing in cases of unlawful/unfair processing. Data subjects must make such a request in writing and, where their request is refused, can apply to the Court for an order for rectification/erasure. All requests will be managed by the Trust's Data Protection Officer.

4.4 The Right to Erasure

Also known as the 'right to be forgotten'. This is to enable an individual to request the deletion or removal of personal data in specific circumstances where there is no compelling reason for its continued processing. All requests must be made in writing to the Trust's Data Protection Officer.

4.5 The Right to Restrict Processing

Individuals have the right to block or suppress processing of personal data. The Trust is permitted to store the personal data when processing is restricted but not further process it.

4.6 The Right to Data Portability

This allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows moving, copying or transferring personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data an individual has provided to a controller;
- where the processing is based on the individual's consent or for the performance of a contract; and
- when processing is carried out by automated means.

4.7 The Right to Object

Individual have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority
- direct marketing
- processing for purposes of scientific/historical research and statistics.

4.8 Rights in Relation to Automated Decision Making and Profiling

The Trust does not carry out any processing operations that constitute automated decision making.

5. Responsibilities

5.1 The Board of Directors

The Trust Board has responsibility for:

- Approving and reviewing this policy via delegation to the People Committee
- Ensuring the implementation of the regulation, its policies, procedures and practices via delegation to the Chief Executive and Chief Operating Officer.

5.2 The Chief Executive

Through delegation from the Board of Directors, ensuring the implementation of the regulation, this policy and the supporting processes, including:

- Ensuring that appropriate training takes place for all staff.
- Ensuring that complaints about the handling of personal data are investigated and dealt with effectively.

5.3 The Data Protection Officer

The role of the Data Protection Officer is:

- to inform and advise the organisation and its employees about their obligations to comply with the GDPR and other data protection laws.
- to monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits.
- to be the first point of contact for supervisory authorities and for individuals whose data is processed (employees etc).
- to coordinate annual training for all staff.

To provide for the independence of the Data Protection function, the Data Protection Officer has a direct right of access to the Chair of the Board of Directors and the Chief Executive, to whom all significant concerns relating to data protection and the GDPR are reported.

The Data Protection Officer will ensure that:

- the Trust and its Academies are appropriately registered with the Information Commissioner's Office and ensure that any changes required to the registration are implemented.
- this policy is implemented in the Trust and Academies' procedures and practices.

- the processes for managing complaints, Subject Access Requests and Freedom of Information requests are properly managed.
- this policy is brought to the attention of all employees, data subjects and that all staff, including temporary, volunteer, supply and agency personnel, receive appropriate training.
- good practice is encouraged by all staff and any breaches of the Regulation and this policy are dealt with appropriately.
- advice and guidance on the aspects of current data protection legislation are provided.

5.4 Executive Team

Each member of the Executive Team is responsible for:

- Documenting data records and processes for their individual areas.
- Ensuring staff training and awareness in data protection for their individual areas, supported by the Data Protection Officer.

5.5 Heads of Academy

Each Head of Academy has overall responsibility and are held accountable for the implementation of this policy and associated data protection procedures.

Heads of Academy are responsible for:

- Ensuring this policy is implemented in Academy procedures and practices.
- Ensuring the associated Trust policies and procedures governing the use, storage and disposal of data are adhered to and reporting any variances to the Data Protection Officer.
- Ensuring positive engagement in staff training.
- Ensuring the Academy completes a privacy notice and displays it on their website.
- Ensuring staff carry out data privacy impact assessments when implementing new ways of processing data. If wishing to purchase new software or systems which process personal data the support of the IT Services Team must be sought prior to purchase / use.

5.6 Data Protection Leads

Each Academy (or central service area) must appoint a Data Protection Lead. The Data Protection Lead is responsible for:

- With the support of the Data Protection Officer coordinate local data protection procedures, ensuring compliance with this policy.
- Maintain the local privacy notice.
- Support staff in completing data privacy impact assessments.
- Support the Data Protection Officer in responding to subject access requests.
- Support the Data Protection Officer in managing data breeches.

5.7 All Staff

All staff have a duty to observe and follow the principles of the GDPR Regulation. These

guidelines are intended to assist staff to understand the aims and principles of the regulation and to set out the main areas in which staff are likely to be affected by data protection issues in the course of their work.

All staff must participate in the online data protection training and complete the model within the agreed timeframe. Records of completion will be kept for logging purposes. Staff must ensure they understand how their work is affected by the Regulation and abide by the principles of the Regulation when processing any personal data. All staff must assess the information used in the course of their work and their responsibility for any personal data. All personal data collected should be factually accurate and relevant. Staff must respect that all sensitive data must be kept confidential and that any breaches of that confidentiality may result in legal action or a possible fine.

All staff must be aware of and ensure that they comply with this Policy. Consequences of non-compliance may include appropriate disciplinary or legal action being taken against the Trust, the Academy and/or the member of staff. A fine could be imposed and reputational loss could ensue as consequences of any negative publicity, particularly if a complaint is made to the ICO or an individual makes a claim for compensation against the organisation.

All contractors and volunteers employed by the Trust who have access to personal data are required to comply with this policy and its supporting policies as specified in the Data Protection schedule of their contract.

6. Access to Information

All individuals about whom the Trust or Academy holds personal information have the right to access information that relates to them, whether it is held electronically or in manual form.

A data subject is entitled to request a copy of the information related to her/him which will be supplied by the Trust or Academy unless the supply is not possible or would involve disproportionate effort.

The right of access extends to children and young people who understand what it means to exercise that right.

The GDPR states that, if consent is the basis for processing a child's personal data, a child under the age of 13 cannot give that consent themselves and instead, consent is required from a person holding 'parental responsibility'.

The Trust/Academy will comply with Freedom of Information Requests as defined in the Trust's Freedom of Information Procedure.

For Subject Access Requests for personal information, the Trust/Academy will ensure that requests for access are dealt with within the timescale specified by legislation. The Trust's Data Subject Access Request Procedure (Annex C) provides detailed guidance about how requests should be dealt with.

7. Records Management

In order to fully understand and manage the information held by the Trust, in order to protect it and

be able to exploit its potential, an Information Asset Register (IAR) will be implemented as a simple way to manage the organisation's assets and the risks to them.

Through its Record Management Policy, the Trust will ensure the systematic management, use and disposition of all records and the information they contain throughout their lifecycle. Effective records management ensures that a body of reliable evidence can be called upon by the Trust if required to justify any actions, or defend its position and to demonstrate its accountability and good standards of corporate governance.

8. Disclosure of Personal Data

The following attempts to illustrate when personal data can be disclosed. This list is not exhaustive and, if further guidance is required, staff should contact their Data Protection Lead or the Trust's Data Protection Officer.

Staff Who Need to Know

Access to personal data will be provided to members of staff who need to know it in order to carry out their normal duties. However, only access to the data that is required will be provided.

Purposes Specified

Data will only be disclosed for use for the purposes specified when it was collected and any additional purpose of which the data subject has been notified. Any other use amounts to unlawful processing.

Specific Agreement of Data Subject

Data subjects should be made aware, via the relevant Privacy Notice, that their personal data may be disclosed to various third parties, without needing specific consent, during the normal course of business activities.

Data may be used for other purposes such as Ofsted Inspections or other governmental/regulatory activity, accounting and statistical analysis, Internal and External Audit and to prevent or detect fraud or other crimes for example. In all other cases, data will only be disclosed to a third party if the data subject has given specific consent, ideally in writing.

Telephone Enquiries: Home Addresses and Telephone Numbers

Requests from third parties are often made by telephone, giving the added problem of verifying the identity of the caller. Even when the call appears to be genuine, personal data must not be disclosed (save where necessary for one of the purposes mentioned above and where the identity of the caller, purpose of the enquiry and proposed use of the information have been verified).

Where appropriate, the caller will be asked to put their request in writing or an offer will be made to contact the data subject concerned, on behalf of the caller and pass on any message.

Home addresses or personal telephone numbers of staff or other data subjects must not be given out to third parties unless the individual has given permission to do so.

Alternative approaches include taking the caller's contact details and advising that a message will be passed on requesting that the caller is contacted, or offering to forward correspondence to a pupil or a member of staff on behalf of the caller.

It is important to take care when handling such requests. An individual's pupil/staff status is personal data. The Trust or Academy should be careful to neither confirm nor deny that the person is a pupil or member of staff at the Academy or that the person is otherwise known to the Trust or Academy.

Law Enforcement Agencies

Disclosures to the Police are not compulsory except in cases where the Trust or Academy is served with a Court Order requiring information. Requests from the Police for access to information must be made, in writing, from one of the Constabulary's Data Protection officers. In cases where the Trust or Academy has not been served with a Court Order but receives a request, consideration must be given to the implications of disclosure before any action is taken and to the nature of the information sought and the reasons for the request. Advice should be sort from the Data Protection Officer.

The Trust or Academy may be required to provide an explanation for any disclosure of the Data Subject's personal information at a later date and must be able to provide justifiable reasons for doing so, for example where the Trust or Academy believes that failure to release the information would prejudice a criminal investigation. In such cases the Data Protection Officer must make a clear and accurate record of the circumstances, the advice sought and the decision-making process followed so that there is clear evidence of the reasoning and the prevailing circumstances. The GDPR Regulation allows organisations to disclose personal data where necessary relating to criminal convictions and offences under the control of official authority or when processing is authorised by state law providing for appropriate safeguards for the rights and freedoms of data subjects.

Education Records

All requests for the data held in Education Records by pupils or parents/legal guardians are treated as a Data Subject Access Request and must be managed by the Data Protection Lead and Data Protection Officer.

All requests for data from third parties must conform to the principles of the GDPR Regulation and must be covered with a Data Sharing Agreement. All Data Sharing Agreements taken out by the Trust or Academy must undergo a Privacy Impact Assessment and the results of the assessment to be kept on file with the Data Sharing Agreement.

Examination Results

Each Academy must ensure that strict confidentiality and secure office practices are followed while papers, including examination coursework, are being marked and while results are being compiled.

The GDPR Regulation does not give pupils the right to access their own examination scripts but it does allow access to comments made upon them by examiners. However, pupils are able, under subject access rights, to see the breakdown of marks awarded for particular questions or sections of examinations.

Examination marks should not be shared, either verbally or in writing, with any other person unless the individual pupil has given their permission e.g. the displaying of examination results on a Academy notice board or a list sent around the classroom is prohibited. Exceptions are other Trust or Academy staff relevant to their role, Ofsted and the DfE.

Photographs and Films

Where it is wished for photographs to be taken or film recordings to be made of staff and/or pupils, as individuals, as small groups or organised groups, the individual(s) concerned must give their consent and be informed of the purpose(s) for which the information is to be used. For pupils under the age of 13, a consent form is given for completion by parents in all Trust Academies at the point of entry. If this form is not completed and returned to the Academy, it is assumed the Trust/Academy does not have consent to photograph or film that pupil. Even if the Trust/Academy does receive consent, we will not photograph or film a pupil if they do not wish to take part on the day.

Once a pupil reaches the age of 13, under Regulation guidelines, consent will be sought from them personally.

For general photographs or video recordings of the Academy grounds and public places, whereby individuals cannot be identified, consent is not required.

A parent may change their mind about consent, even after signing the above consent form but they must inform the Academy that they wish to withdraw their child from photographs or filming. Likewise, a pupil aged 13 or over may change their mind about consent but must inform the Academy.

Photos/films of pupils may be kept and used after a pupil has left an Academy but only for the original purpose(s) stated in the signed consent form. If the Trust wish to use photos / films for a different purpose to that which was originally explained to the pupils in question, renewed consent will need to be sought, regardless of whether or not the pupil is still at the Academy.

Parents are reminded that, if they attend an Academy event, they should only take photographs of or film their own child(ren) unless they seek the consent of other children's parents/guardians.

All images will be stored securely and safely and Academies will be expected to delete images after a reasonable time has passed.

Please refer to the Trust Media Protocol for further information.

CCTV

Each Academy must ensure any recorded images are stored securely and in a location/on a medium where only authorised persons have access to them. The recorded images must only be retained long enough for any incident to come to light (e.g. for a theft to be noticed). The Academy may disclose recordings to a law enforcement agency in order to help with the prevention or detection of crime but must not release the images to any other third party.

Equal Opportunities Monitoring

The GDPR Regulation specifically allows for processing of data on racial or ethnic origin, religion and disability if it is necessary for keeping under review the existence, or absence, of

equality of opportunity. The collection of this information is exclusively used for the statistical evaluation of the Trust's equal opportunities policy within recruitment and employment.

The Trust, where possible, will ensure anonymity of information when meaningful monitoring is required. The equal opportunities monitoring form, which collects information for this purpose, must be removed from all applications before any assessment of suitability for the post is considered.

Websites

Data placed on the Trust's or an Academy's website and made available via the Internet will be available in countries which do not have a data privacy regime considered adequate by the EU. Where the Trust or Academy wishes to make staff/pupil personal data available in this way, the consent of the staff and/or pupil(s) concerned must be obtained. Consent can be withdrawn at any point.

Website pages are sometimes used to collect personal data such as names and addresses of individuals who request Trust or Academy information e.g. from those who are registering to attend an Open Day. The relevant web page should indicate the purpose or purposes for which the data is collected, the recipients to whom it may be disclosed and an indication of the time period for which it will be kept (e.g. "while we process your application", rather than a specific date).

All sites that collect information from site visitors must provide a Privacy Statement. The purpose of this statement is to help individuals to decide whether they want to visit the site and, if so, whether to provide any personal information. Privacy Statements must be prominently displayed.

The above does cover all requirements and consideration must be given to the intended audience and the use their data may be put to deliver Trust obligations.

Annex A – Contact Details

Trust Data Protection Officer	Wayne Oldfield, Chief Operating Officer The Boston Witham Academies Federation Trust Offices Marian Road Boston Lincolnshire PE21 9HB Tel: 01205 319503 Email: dpo@bwaf.net
Information Commissioners Office	Information Commissioner's Office Wycliffe House Water Lane Wilmslow Cheshire SK9 5AF Tel: 0303 123 1113 Web: https://www.ico.org.uk

Annex B – Definitions

Automated data	Data which is processed by means of equipment operating automatically (e.g. by computer) or which is recorded with the intention that it should be so processed.
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
Consent	Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Data	Information which is processed automatically or recorded manually.
Data Controller	The natural or legal entity which determines the purposes and means of processing personal data. The Boston Witham Academies Federation (the Trust) is the Data Controller.
Data Privacy Impact Assessment	A DPIA is a process to help organisations identify, assess and mitigate or minimise privacy risks with data processing activities – for example, the launch of a new product or the adoption of a new practice or policy or system.
Data Subject Access Request	A request by a Data Subject for details of the personal data held about them.
Data Subject	A natural person whose personal data is processed by a controller or processor.
Data Protection Officer	A Data Protection Officer (DPO) is a leadership role required by the General Data Protection Regulation (GDPR) and is responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR requirements. The Chief Operating Officer is the Trust's Data Protection Officer.
Data User	Someone who controls the collection, holding, processing or the use of data.
Explicit consent	Explicit consent is that which must be affirmed by the individual in an informed, clear and specific statement, preferably in writing, specifying the purposes for which the particular types of sensitive personal data may be used and/or the countries to which they may be disclosed.
Personal data	Any information relating to an identified or identifiable natural person ('data subject') that can be used to directly or indirectly identify that person.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Privacy Notice	A statement made to a data subject that describes how the organisation collects, uses, retains and discloses personal information.

Process/processing	Any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, including collection, recording, organisation, structuring, storage, erasure or destruction.
Sensitive personal data	Information concerning a data subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union activities, physical or mental health or condition, sexual life or orientation, genetic data or biometric data.

Annex C - Data Subject Access Request Procedure

The procedure outlines the steps to be followed, the records to be kept and the rules that must be applied. The attached appendices include draft letters to be used when responding to Data subject Access requests.

An application form for use across the Trust is also included in the attached appendices.

Although the GDPR provides for Data Subject Access Requests, it is not necessary to follow this procedure for every request for information. If a general enquiry is made regarding information held or used in a process, then it should be dealt with as part of normal working practices.

The GDPR only applies to personal information, i.e. information about identifiable living individuals. In the majority of circumstances, the issue will be resolved without reference to the GDPR. If the Data Subject specifically makes the request under the GDPR, then the procedure must be followed.

Rights of the Data Subject

The Data Subject has the right to confirmation as to whether personal data concerning him or her is being processed and, where this is the case, access to the personal data and:

- The purposes of the processing.
- The categories of personal data concerned.
- The recipients to whom the personal data has been or will be disclosed.
- Where possible, the envisaged period for which their personal data will be stored.
- The existence of the right to request rectification or erasure of personal data or restriction of processing concerning the data subject or to object to such processing.
- The right to lodge a complaint with a supervisory authority.
- Where the personal data is not collected from the data subject, any available information as to their source.
- The existence of automated decision making, i.e. where their data is processed automatically and is likely to form the sole basis for any decision significantly affecting them.

Obligations

The data subject should:

- Submit a written request for subject access.
- Provide satisfactory proof of identity and address e.g. driving licence, council tax or utility bill.
- Provide sufficient information to enable the data to be located e.g. name, address and relevant reference numbers.

The data user should:

- Be satisfied as to the identity of the Data Subject.
- Obtain sufficient information to enable the data to be located.
- Inform the Data Subject whether data are held about them.
- Ensure the consent of any third party individual that can be identified from the personal data has been obtained before disclosing that part of the data or take steps to prevent the

disclosure of that data to the Data Subject. Care should be taken to ensure that the identity of the third party source of the data is not revealed.

- Provide the Data Subject with a copy of the personal data which relates to the Data Subject together with an interpretation of any terms or codes used by the Trust or Academy relating to the data.
- Respond within fifteen (15) school days of receipt of written request for subject access in relation to requests for educational records and within one calendar month days for all other information requested.
- Provide an initial response to the requester within twenty-one (21) calendar days of receiving an access request, confirming the request is being complied with and indicating the intention to comply or giving reasons for not complying with the request.
- Retain a copy of the information supplied (for use in case of the information being challenged).
- Implement a method to log subject access requests, to enable the progress of such requests to be monitored and to produce statistics.

Types of Request

There are three types of request likely to be received by the Trust:

- Routine requests for information which can be satisfied without recourse to the GDPR, e.g. can I have a copy of the letter I sent you last week?
- Requests for information which the Data Subject has the right to see under laws and policies other than the GDPR.
- Formal requests for access to information under the GDPR. e.g. Can I have the details you hold about me?

Requests received in the format of points 1 and 2 above must be processed in accordance with this procedure on handling requests, although in some cases it may be prudent to treat these requests as subject access requests under the GDPR and apply the necessary controls.

It is intended that the Data Subject should complete a standard application form (Annex D) when requesting subject access. The standard form can be sent to the Data Subject on request. An applicant's own written request is acceptable if it provides the information required to enable the data to be located. When the necessary information has been received from the Data Subject, the request must be processed as outlined in the following procedure.

The Standard Form should be either posted to the Trust's Data Protection Officer using the address in Annex B or Emailed to dpo@bwaf.net.

Charges

A fee may not usually be charged for dealing with a SAR. However, there are different fee structures for organisations that hold health or education records (where the maximum fee is £50, depending on the circumstances – see ICO Code of Practice). These fees are not subject to VAT. If a fee is charged, a request need not be complied with until the fee has been received

You need not comply with a request until a fee has been received but a request cannot simply be ignored because the individual has not sent a fee. If a fee is payable but has not been sent with the request, the individual should be contacted promptly and informed that they need to pay.

Receiving a Request

The request is received from the Data Subject at any Academy or Trust office in either letter format or on a standard Data Subject request form (Annex D). It must not be accepted as a verbal request.

The request should be forwarded by the Data User to the Trust's Data Protection Officer (DPO) immediately.

Verify the Request

The request should be checked to verify that it has been completed correctly and that all information relevant for the request has been given i.e. payroll number, pass type and number.

If the application form/letter does not contain all the information necessary to carry out the request, a letter, requesting additional information, along with the original application must be sent to the applicant. Details of the request should still be recorded in the subject access log.

An applicant cannot request information on behalf of another individual unless written authorisation has been obtained from the Data Subject. This authorisation must be verified and, where necessary, identification of the applicant must be obtained. In all cases, however, the information must be sent to the Data Subject.

Where an individual has power of attorney, proof must be obtained, and in this case, the data must be sent to that individual.

Log the Request

If the request has been received before (i.e. returned to the applicant for more information) the subject access log should be updated to reflect this. Otherwise the details of the request should be recorded in the subject access log. When a valid request has been received, a letter of acknowledgement must be sent to the applicant and the Data Protection Lead will be informed.

Process the Request

The details of the Data Subject will be retrieved into a format suitable for presenting to the applicant. This should include definitions of any codes/references where the explanation is not apparent.

Any information sent to the Data Subject should not include any data about, or such that it would allow the Data Subject to identify any third party unless permission has been sought and received from that individual. Care must be taken to ensure that the identity of a third party is not disclosed by either blanking out their names/addresses/identification or providing the information in another format i.e. typed. The only exception to this rule is where other legislation forces you to release that information.

Information held for the prevention and detection of a crime e.g. fraud or information being used for a case currently under investigation does not need to be disclosed. However, once the investigation has been completed, then the information must be released if a Data Subject requests access to their data.

A copy of all the data retrieved must be taken for reference should the data be challenged by the Data Subject and shall become part of the subject access log.

Provide the Data

An appointment should be arranged by the Data Protection Lead with the Data Subject where it would be preferable or necessary to explain the information or when the Data Subject has requested a meeting to discuss the details of his/her request.

If an appointment is not necessary, the information along with a letter and any other guidance should be sent to the Data Subject.

The information may be sent to the Data Subject as a computer print-out, in a letter or on a form. However, the data must be in a format that will be understood by the Data Subject with an explanation of any codes that have been used. The information must be provided to the applicant within one calendar month of receiving a valid request, i.e., all the information necessary to process it and within fifteen (15) school days in the case of a valid request for educational records.

If data could not be found to satisfy the application, a letter must still be sent to the Data Subject stating this.

Closing the Request

When all details have been passed to the applicant, the subject access log must be updated accordingly.

Appeals Procedure

If the Data Subject is not satisfied with the information provided and has notified the Trust to this effect, the Data Protection Officer will consider the request and deal with it accordingly.

Details to be Recorded

The following details should be recorded in the subject access log. This will enable the progress of requests to be monitored and will allow statistics to be produced.

- Reference number (given by the DPO)
- Name and address of Data Subject
- Name and address of applicant (if not the same as the Data Subject)
- Date the request was received
- Date the valid request was received (may be the same as above)
- Date the request was returned to applicant for further details
- Date the request must be completed by (ie, one calendar month after valid request received) or fifteen (15) school days in respect of Educational records
- Department/Academy dealing with request
- Name of person dealing with request
- Date the letter of acknowledgement was sent
- Date request completed and information passed to applicant
- Comments
- Details of proof of identity
- Type of information requested i.e. payroll, personnel details, etc.
- Copy of the information provided to applicant

Annex D – Data Subject Access Request Form

Data Subject's Name	
Address	
Previous address if you have moved since your details were given to the Boston Witham Academies Federation	
Your Name (if you are not the data subject*)	
Your Address	
Please state what information you require and the reasons why The Boston Witham Academies Federation would have personal information about the Data Subject in its files. Details of any reference number e.g. payroll, pass type and number and any specific information which will assist us to process your application.	

Signed		**Signed**	
Date		**Date**	

*You will need written authorisation from the Data Subject before this application can be processed.

Guidance for the Applicant

To enable your request for access to be processed promptly, please complete this form, providing as much information as you can.

You will be asked to provide satisfactory proof of identity and address e.g. driving licence, passport, recent correspondence addressed to you.

If you are requesting access on behalf of another individual, you will be required to provide written authorisation from the Data Subject. Any data found will be sent to the Data Subject.

Guidance for the Receiving Office

Upon receipt of this form from the applicant please complete the section below.

Location Received	
Date Received	
Received By	
Job Title	
Type of Identification Submitted by Applicant	
Reference Number of Application	
Request Type	Pupil ☐ Employee / Former Employee ☐ Supplier / Contractor ☐ Public ☐

Once completed please scan and send the form and all supporting documents to dpo@bwaf.net for processing. This form must be sent to the Data Protection Officer on the day it is received at the appropriate office.

Annex E – Data Security Breach Procedure

Introduction

The Trust holds a large amount of data / information, both in hard and soft copy. This includes personal or confidential information (about people) and also non-personal information which could be sensitive or commercial, for instance financial data.

Care should be taken to protect this type of data / information to ensure it is not changed (either accidentally or deliberately), lost, stolen or falls into the wrong hands and that its authenticity and integrity is maintained.

In the event of a breach, it is vital that appropriate action is taken to minimise associated risks.

What is a Breach?

A data breach is an incident in which any of the types of data specified above is compromised, disclosed, copied, transmitted, accessed, stolen or used by unauthorised individuals, whether accidentally or on purpose. Some examples are:

- Accidental loss or theft of equipment on which data is stored
- Unauthorised access to data
- Human error such as emailing data by mistake
- Failure of equipment and hence data held on it
- Loss of data or equipment through fire or flood, for example
- Hacking attack
- Where information is obtained by deceiving a member of staff

A personal data breach is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means a breach is more than just losing personal data.

Reporting a Breach

Data security breaches should be reported immediately to the Trust's Data Protection Officer as the primary point of contact. The report should include full and accurate details of the incident, including who is reporting the incident, what type of data is involved, if the data relates to people, how many people are involved.

The Data Protection Officer will keep a log of this information. If a breach occurs out of Academy hours, you must notify the Data Protection Officer as soon as is physically possibly.

The Data Protection Officer's contact details are:

Tel: 01205 319503
Email: dpo@bwaf.net

You must also notify your Head of Academy and Data Protection Lead immediately.

Investigation and Risk Assessment

The Data Protection Officer will instigate a Data Emergency Response Team (DERT), who will be responsible for investigating data breaches. An investigation will be started within twenty-four (24) working hours of the breach being discovered.

Depending on the type of breach, DERT members may consist of:

- the Data Protection Officer
- the Head of Academy
- the Data Protection Lead
- the IT Manager
- Data Users
- Executive Team Members

The investigation will establish the nature of the breach, the type of data involved, whether the data is personal data relating to individuals and, if so, who are the subjects and how many are involved.

The investigation will consider the extent of the sensitivity of the data and a risk assessment performed as to what might be the consequences of its loss, for instance whether harm could come to individuals or to the institution.

On completion of the investigation, a report will be completed within ten (10) working days.

Containment and Recovery

DERT will determine the appropriate course of action and the required resources needed to limit the impact of the breach. This might require isolating a compromised section of the IT Network, alerting relevant staff or shutting down critical equipment.

Appropriate steps will be taken to recover data losses and resume normal business operation. This might entail attempting to recover any lost equipment, using backup mechanisms to restore compromised or stolen data and changing compromised passwords.

Notification

The Chief Executive will be notified by the Data Protection Officer following a critical data breach involving large amounts of data or a significant number of people whose personal data has been breached. They, along with the Data Protection Officer, will make a decision to notify the Board of Directors based on the seriousness of the breach.

The Chief Executive, along with the Data Protection Officer, will make a decision to inform any external organisation such as the police or other appropriate regulatory body.

If a personal data breach has occurred, the Data Protection Officer must inform the Information Commissioner's Office within seventy-two (72) hours of notification of the breach.

Notice of the breach will be made to affected individuals to enable them to take steps to protect themselves. This notice will include a description of the breach and the steps taken to mitigate the risks and will be undertaken by the Trust.

Review

Once the breach is contained, a thorough review of the event will be undertaken by DERT to establish the cause of the breach, the effectiveness of the response and to identify areas that require improvement.

Recommended changes to systems, policies and procedures will be documented and implemented as soon as possible thereafter.