

South Bank Multi Academy Trust

GDPR Information Governance (Data Protection) Policy

Approved by Trustees: January 2022

Version: 2.0

Review Timetable: 3 years

Renewal Date: January 2025

1. INTRODUCTION

- 1.1 This policy is to ensure that South Bank Multi Academy Trust (SBMAT) complies with the requirements of the General Data Protection Regulation, Environmental Information Regulations 2004 (EIR) and Freedom of Information Act 2000 (FOIA), associated guidance and Codes of Practice issued under the legislation.

2. SCOPE

- 2.1 The Information Policy applies to information in all forms including, but not limited to:
- Hard copy or documents printed or written on paper;
 - Information or data stored electronically, including scanned images;
 - Communications sent by post/courier or using electronic means such as email, fax or electronic file transfer;
 - Information or data stored on or transferred to removable media such as tape, CD, DVD, USB storage device or memory card;
 - Information stored on portable computing devices including mobile phones, tablets, cameras and laptops;
 - Speech, voice recordings and verbal communications, including voicemail;
 - Published web content, for example intranet and internet;
 - Photographs and other digital images.
- 2.2 This policy is the Trust's main information governance policy and addresses:
- Data protection (including rights and complaints)
 - Freedom of information

- Information asset management

2.3 Information security, acceptable use of systems, records management and security incident reporting will be addressed in separate policies.

3. DATA PROTECTION

- 3.1 Personal data will be processed in accordance with the requirements of the UK GDPR and in compliance with the data protection principles specified in the legislation.
- 3.2 The Trust has notified the Information Commissioner's Office that it is a Data Controller and has appointed a Data Protection Officer (DPO). Details of the DPO can be found here.

Schools Data Protection Officer
Veritau Ltd
County Hall
Racecourse Lane
Northallerton
DL7 8AL

schoolsDPO@veritau.co.uk
01904 554025

Please ensure you include the name of your school in all correspondence



- 3.3 The DPO is a statutory position and will operate in an advisory capacity. Duties will include:
- Acting as the point of contact for the Information Commissioner's Office (ICO) and data subjects;
 - Facilitating a periodic review of the corporate information asset register and information governance policies;
 - Assisting with the reporting and investigation of information security breaches
 - Providing advice on all aspects of data protection as required, including information requests, information sharing and Data Protection Impact Assessments; and
 - Reporting to the Trust Board and Local Governing Body on the above matters.

4. Information Asset Register

- 4.1 The DPO will advise the Trust in developing and maintaining Information Asset Registers (IAR) for each of its schools. The registers will include the following information for each asset:

- An individual information asset identification number;
- The owner of that asset;
- Description and purpose of the asset;
- Whether there is a privacy notice published for that asset;
- Format and location of the asset;
- Which officers (job titles/teams) have routine access to the information;
- Whether there are any data sharing agreements relating to the information and the name of that agreement,
- Conditions of data processing;
- Details of any third parties contracted to process the information;
- Retention period for the asset

4.2 The IAR will be reviewed annually and the School Finance / Business Manager will inform the DPO of any significant changes to their information assets as soon as possible.

5. Information Asset Owners

- 5.1 An Information Asset Owner (IAO) is the individual responsible for an information asset, understands the value of that information and the potential risks associated with it. The Trust will ensure that IAO's are appointed based on sufficient seniority and level of responsibility.
- 5.2 IAO's are responsible for the security and maintenance of their information assets. This includes ensuring that other members of staff are using the information safely and responsibly. The role also includes determining the retention period for the asset, and when destroyed, ensuring this is done so securely.

6. Training

- 6.1 The Trust will ensure that appropriate guidance and training is given to the relevant staff, governors and other authorised school / Trust users on access to information procedures, records management and data breach procedures. Individuals will also be made aware and given training in relation to information security including using email and the internet.
- 6.2 The DPO will provide the Trust with adequate training resources and guidance materials. The DPO will be consulted, and will offer an adequacy opinion if the Trust opts to use a third party provider.
- 6.3 The Trust will maintain a "training schedule" which will record when employees have completed an information governance training module and when a refresher is due to be completed.

- 6.4 The school / Trust will ensure that any third party contractors have adequately trained their staff in information governance by carrying out the appropriate due diligence.

7. Privacy Notices

- 7.1 Each school will provide a privacy notice to data subjects each time it obtains personal information from or about that data subject.
- 7.2 Our main privacy notice will be displayed on the school's / Trust's website in an easily accessible area. This notice will also be provided in a hard copy to pupils and parents at the start of their time with the school within their information pack.
- 7.3 A privacy notice for employees will be provided at commencement of their employment with the Trust. Specific privacy notices will be issued where the data subject requires more information about specific processing (e.g. school trips, projects).
- 7.4 Privacy notices will be cleared by the DPO prior to being published or issued. A record of privacy notices shall be kept on the school's Information Asset Register.

8. Information Sharing

- 8.1 In order to efficiently fulfil our duty of education provision it is sometimes necessary for the Trust to share information with third parties. Routine and regular information sharing arrangements will be documented in our main privacy notice (as above). Any ad hoc sharing of information will be done in compliance with our legislative requirements.

9. Data Protection Impact Assessments (DPIAs)

- 9.1 The school / Trust will conduct a data protection impact assessment for all new projects involving high risk data processing as defined by GDPR.
- 9.2 This assessment will consider the privacy risks and implications of new projects as well as providing solutions to the identified risks
- 9.3 The DPO will be consulted at the start of a project and will advise whether a DPIA is required. If it is agreed that a DPIA will be necessary, then the DPO will assist with the completion of the assessment, providing relevant advice.

10. Retention Periods

- 10.1 Retention periods will be determined by any legal requirement, best practice or national guidance, and lastly the organisational necessity to retain the information. In addition IAOs will take into account the Limitation Act 1980, which provides timescales within which action may be taken for breaches of the law, when determining retention periods.

10.2 The Trust has opted to adopt the retention schedule suggested by the Information and Records Management Society (IRMS).

11. Destruction of Records

- 11.1 Retention periods for records are recorded in the school's IAR. When a record reaches the end of its retention period the IAO will arrange for the records, both electronic and paper to be destroyed securely. Provisions to destroy paper information securely include cross cutting shredders and confidential waste bins.
- 11.2 Advice in regards to the secure destruction of electronic media will be sought from relevant IT support.
- 11.3 A record should be retained of all files destroyed including, where relevant:
- File reference number,
 - Description of file,
 - Date of disposal,
 - Method of disposal,
 - Officer who destroyed record

12. Third Party Data Processors

- 12.1 All third party contractors who process data on behalf of the school must be able to provide assurances that they have adequate data protection controls in place to ensure that the data they process is afforded the appropriate safeguards. Where personal data is being processed, there will be a written contract in place with the necessary data protection clauses contained.
- 12.2 Relevant senior leadership may insist that any data processing by a third party, ceases immediately if it believes that that third party has not got adequate data protection safeguards in place. . If any data processing is going to take place outside of the EEA then the Data Protection Officer must be consulted prior to any contracts being agreed.

13. Access to Information

Requests for information under the Freedom of Information Act 2000 (FOIA) and Environmental Information Regulations 2004 (EIR)

- 13.1 **Requests under this legislation should be made to either the Trust or an individual school and for the attention of the Trust / School Finance / Business Manager**
- 13.2 The Trust / School Finance / Business Manager is responsible for:
- Deciding whether the requested information is held;
 - Locating, retrieving or extracting the information;

- Considering whether any exemption might apply, and the balance of the public interest test;
- Preparing the material for disclosure and drafting the response;
- Seeking any necessary approval for the response; and
- Sending the response to the requester

- 13.3 FOIA requests should be made in writing. Please note that we will only consider requests which provide a valid name and address and we will not consider requests which ask us to click on electronic links. EIR requests can be made verbally, however we will endeavour to follow this up in writing with the requestor to ensure accuracy.
- 13.4 Each request received will be acknowledged within 5 working days. The Chair of Governors / Chair of the Board of Trustees and Trust Principal / Headteacher will jointly consider all requests where a public interest test is applied or where there is any doubt on whether an exemption should be applied. In applying the public interest test they will:
- Document clearly the benefits of both disclosing or withholding the requested information; and
 - Where necessary seek guidance from previous case law in deciding where the balance lies
 - Consult the DPO
- 13.5 Reasons for disclosing or not disclosing will be reported to the next Local Governing Body and / or Trust Board meeting.
- 13.6 We have adopted the Information Commissioner's model publication scheme for schools and will publish as much information as possible on our website in the interests of transparency and accountability.
- 13.7 We will charge for supplying information at our discretion, in line with current regulations. If a charge applies, written notice will be given to the applicant and payment must be received before the information is supplied. Any charges will be formulated taking into account the limits set by the legislation.
- 13.8 We will adhere to the required FOI/EIR timescales, and requests will be answered within 20 **working days**.

Requests for information under the UK GDPR- Subject Access Requests

- 13.9 **Requests under this legislation should be made to either the Trust or an individual school and for the attention of the Trust / School Finance / Business Manager**

- 13.10 Any member of SBMAT's staff including Governors and Trustees may receive a request for an individual's personal information. Whilst the UK GDPR does not require such requests to be made in writing, applicants are encouraged where possible to do so; applicants who require assistance should seek help from the school. Requests will be logged with the Finance / Business Manager and acknowledged within 5 working days.
- 13.11 We must be satisfied as to your identity and may have to ask for additional information such as:
- Valid Photo ID (driver's licence, passport etc);
 - Proof of Address (Utility bill, council tax letter etc);
 - Further information for the school to be satisfied of the applicant's identity;
- 13.12 Only once the school / Trust is satisfied of the requestor's identity and has sufficient information on which to respond to the request, will it be considered valid. We will then respond to your request within the statutory timescale of One Calendar Month.
- 13.13 The school / Trust can apply a discretionary extension of up to a further Two Calendar Months to comply with the request if the requested information would take a considerable amount of time to collate, redact, and prepare for disclosure due to either the complexity or voluminous nature of the records. If we wish to apply an extension we will firstly seek guidance from our DPO, then inform the applicant of the extension within the first calendar month of receiving the request. This extension period will be kept to a minimum and will not be used as a way of managing workloads. In very limited cases we may also refuse a request outright as 'manifestly unreasonable' if we would have to spend an unjustified amount of time and resources to comply.
- 13.14 Should we think any exemptions are necessary to apply we will seek guidance from our DPO to discuss their application.

For secondary settings: If a subject access request is made by a parent whose child is 12 years of age or over we may consult with the child or ask that they submit the request on their own behalf. This decision will be made based on the capacity and maturity of the pupil in question.

Requests received from parents asking for information held within the pupil's Education Record will be dealt with under the Education (Pupil Information) (England) Regulations 2005. Any charges which arise from this request will be applied at our discretion.

14. Data Subject Rights

- 14.1 As well as a right of access to information, data subjects have a series of other rights prescribed by the UK GDPR including:
- Right to rectification
 - Right to erasure
 - Right to restrict processing
 - Rights in relation automated decision making and profiling
- 14.2 All requests exercising these rights must be in writing and forwarded to the school the request is concerning, and for the attention of the School Finance / Business Manager who will acknowledge the request and respond within One Calendar Month. Advice regarding such requests will be sought from our DPO.
- 14.3 A record of decisions made in respect of the request will be retained, recording details of the request, whether any information has been changed, and the reasoning for the decision made.

15. Complaints

- 15.1 Complaints in relation to FOI/EIR and Subject Access will be handled through our existing procedures. Any individual who wishes to make a complaint about the way we have handled their personal data should contact the DPO on the address provided.

16. Copyright

- 16.1 South Bank Multi Academy Trust will take reasonable steps to inform enquirers if any third party might have a copyright or intellectual property interest in information provided in response to their requests. However it will be the enquirer's responsibility to ensure that any information provided by the school is not re-used in a way which infringes those interests, whether or not any such warning has been given.