Data Protection & Freedom of Information Policy

Reviewed: April 2018
Next Review Date: April 2019

The Bay Learning Trust
The Lodge
Ripley St Thomas
Ashton Road
Lancaster
LA1 4RR

t 01524 581872
e admin@baylearningtrust.com
website baylearningtrust.com

1. Compliance

1.1. This policy has been prepared with due regard to the following statutory provisions:-

1.1.1. Data Protection Act 1998

1.1.2. Freedom of Information Act 2000

2. About this policy

2.1. All schools and are data controllers under the Data Protection Act and have specific duties they must comply with.

2.2. All schools (except independent schools) are public authorities under the Freedom of Information Act 2000.

2.3. This policy sets out the duties of The Bay Learning Trust ("the Trust") under each of the legislation provisions referred to in paragraph 2 of this policy, the responsible bodies/person for compliance and the procedures that will be applied.

2.4. During the course of its activities the Trust will process personal data (which may be held on paper, electronically, or otherwise) about the Trust's staff (including temporary staff), agency workers, volunteers, pupils, their parents, guardians or carers, and other individuals (including suppliers and governors).

2.5. The Trust recognises the need to treat personal data in an appropriate and lawful manner, in accordance with the Data Protection Act 1998 (DPA) and associated Information Commissioner's Office (ICO) Guidance applicable from time to time. The purpose of this policy is to make the data subject aware of how the Trust will handle personal data.

2.6. This policy also outlines the Trust Board's approach to requests made under the Freedom of Information Act 2000 (FOIA).

2.7. The Trust Board complies with the provisions of the FOIA which allows any member of the public to request information from public bodies including Academies created under the Academies Act 2010.

2.8. The Trust Board also complies with ICO and DfE Guidance applicable from time to time.

2.9. This policy does not form part of any employee's contract of employment and may be amended at any time.

3. Who is responsible for this policy

3.1. The Trust Board has overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework for data protection and freedom of information.

3.2. The Trust Board has delegated day-to-day responsibility for operating the policy and ensuring its maintenance and review to the Director of Operations notwithstanding that the Trust is data controller as defined in Section 1 of the DPA and public authority as defined in Section 3 of the FOIA.

3.3. The **Senior Leadership Team** has a specific responsibility to ensure the fair application of this policy and all staff have an individual responsibility to ensure that they understand the implications of the data protection principles (**Principles**) outlined in paragraph 6.1.2 and that the Principles are adhered to.

4. Who is covered by this policy

4.1. This policy covers all staff at all levels and grades including senior managers, employees, trainees, part-time and fixed term employees, permanent, temporary, agency workers and volunteers (referred to as **staff** or **data subject** in this policy).

5. Definitions

5.1. The definitions in this paragraph apply in this policy.

5.2. **Personal data:** means recorded information the Trust holds about a data subject from which he/she can be identified. It may include contact details, other personal information, photographs, expressions of opinion about a data subject or indications as to the Trust's intentions about the data subject.

5.3. **Processing:** means doing anything with the data, such as accessing, disclosing, destroying or using the data in any way.

5.4. **Sensitive personal data:** means data about ethnic origin, political opinions, religious or similar beliefs, trade union membership, health, sex life, criminal proceedings or convictions

6. Data protection and educational records

6.1. Data protection principles

6.1.1. 'Personal data' is defined in Section 1 of the DPA and is information that on its own, or in conjunction with other information the Trust's possession or likely to come into the Trust's possession, identifies the data subject. This includes opinion.

6.1.2. The Trust will comply with the eight data protection principles in the DPA, which require that personal data must be:

6.1.2.1. processed fairly and lawfully;

6.1.2.2. processed for limited purposes and in an appropriate way;

6.1.2.3. adequate, relevant and not excessive for the purpose;

6.1.2.4. accurate;

6.1.2.5. not kept longer than necessary for the purpose;

6.1.2.6. processed in line with individuals' rights;

6.1.2.7. secure; and,

6.1.2.8. not transferred to people or organisations situated in countries without adequate protection.

7. Fair and lawful processing

7.1. The Trust will usually only process personal data where the data subject has given his/her consent or where the processing is necessary to comply with the Trust's legal obligations. In other cases, processing may be necessary for the protection of a data subject's vital interests, for the Trust's legitimate interests or the legitimate interests of others. The full list of conditions is set out in Schedule 2 of the DPA.

7.2. The Trust will only process sensitive personal data where a further condition is also met. Usually this will mean that the data subject has given his/her explicit consent, or that the processing is legally required for employment purposes. The full list of conditions is set out in Schedule 3 of the DPA.

8. How the Trust is likely to use personal data

8.1. Staff

8.1.1. The Trust will process data about staff for legal, personnel, administrative and management purposes and to enable the Trust to meet it's legal obligations as an employer and education provider.

8.1.2. The Trust will process personal data in order to, for example:

8.1.2.1. pay the data subject;

8.1.2.2. monitor performance;

8.1.2.3. provide information on the Trust or and individual Academy's website in order to meet the legitimate needs of visitors to the Trust and/or Academy and enquirers looking to make contact with it;

8.1.2.4. perform recruitment and pre-employment checks;

8.1.2.5. comply with legal obligations under relevant legislation;

8.1.2.6. confer benefits in connection with a data subject's employment.

8.1.2.7. The Trust may process sensitive personal data relating to staff including, as appropriate:

8.1.2.7.1. information about a staff member's physical or mental health or condition in order to monitor sick leave and take decisions as to the staff member's fitness for work;

8.1.2.7.2. the staff member's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; and,

8.1.2.7.3. in order to comply with legal requirements and obligations to third parties.

8.2. **Pupils**

8.2.1. The Trust will process data about pupils for the following (non-exhaustive) purposes:

8.2.1.1. for legal and administrative purposes;

8.2.1.2. to provide education and discharge the Trust's duty of care as an education provider;

8.2.1.3. to provide pupils with a safe and secure environment and pastoral care;

8.2.1.4. to provide activities including school trips, activity and after-school clubs;

8.2.1.5. to provide academic and examination references; and,

8.2.1.6. to enable the Trust to meet the it's legal obligations under relevant legislation and Department for Education (DfE) Guidance in force from time to time.

8.2.2. The Trust will process personal data in order to, for example:

8.2.2.1. maintain educational records;

8.2.2.2. monitor attendance;

8.2.2.3. maintain health and safety records;

8.2.2.4. collect opinions about ability and achievements;

8.2.2.5. obtain and retain details about personal / home life where this is relevant to provision of education to a data subject; and,

8.2.2.6. share information with other agencies when strictly required.

8.2.3. The Trust may process sensitive personal data relating to pupils including, as appropriate:

8.2.3.1. information about pupil's physical or mental health or condition (including but not limited to allergies and regular medications) in order to discharge the Trust's duty of care, provide non-emergency and emergency medical assistance and for special educational needs provision;

8.2.3.2. the pupil's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation or to ensure that religious or similar beliefs are respected; and/or,

8.2.3.3. in order to comply with other legal requirements and obligations to third parties.

8.3. Parents, guardians, carers and other individuals (including suppliers and Governors)

8.3.1. The Trust may process data about parents, guardians, carers and other individuals (including suppliers and governors) for the purpose of:

8.3.1.1. providing education to pupils;

8.3.1.2. maintaining emergency contact details in order to discharge the Trust's duty of care as an education provider;

8.3.1.3. organise training courses;

8.3.1.4. obtain and retain details about personal / home life where this is relevant to provision of education to pupils; and

8.3.1.5. discharge obligations under safeguarding and other relevant legislation.

8.3.1.6. It is very unlikely that the Trust will process sensitive personal data relating to parents, guardians, carers and other individuals (including suppliers and governors). However, where this may be necessary, it may include, as appropriate:

8.3.1.6.1. the parent, guardian, carer or other individual's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation; and/or,

8.3.1.6.2. in order to comply with other legal requirements and obligations to third parties.

9. Processing for limited purposes

9.1. The Trust will only process personal data for the specific purpose or purposes notified to data subjects or for any other purposes specifically permitted by the DPA.

9.2. If staff need to process personal data relating to volunteers, suppliers, pupils, their parents, guardians or carers, and other individuals (including suppliers and governors) outside of the original purpose for which it was acquired, they should seek advice from the MAT Data Protection Officer.

9.3. If staff are unsure about the purpose for which personal data relating to volunteers, suppliers, pupils, their parents, guardians or carers, and other individuals (including suppliers and governors) is being processed, they should seek advice from the MAT Data Protection Officer.

10. Adequate, relevant and non-excessive processing

10.1. Personal data will only be processed to the extent that it is necessary for the specific purposes notified to the data subject.

11. Accurate data

11.1. The Trust will keep the personal data the Trust store about a data subject accurate and up to date. Data that is inaccurate or out of date will be destroyed. Data subjects should notify the Trust if any personal details change or if the data subject becomes aware of any inaccuracies in the personal data the Trust hold about him/her.

12. Data retention

12.1. The Trust will not keep personal data for longer than is necessary for the purpose. This means that data will be destroyed or erased from the Trust's systems when it is no longer required. The Trust has produced a detail schedule of retention periods, which can be found at Annex 1 to this policy.

13. Processing in line with subject access rights

13.1. Data subjects have the right, under the DPA, to:

13.1.1. request access to any personal data the Trust hold about him/her. For pupils, this includes educational records;

13.1.2. prevent the processing of data for direct-marketing purposes;

13.1.3. ask to have inaccurate data held about the data subject amended;

13.1.4. prevent processing that is likely to cause unwarranted substantial damage or distress to the data subject or anyone else; and,

13.1.5. object to any decision that significantly affects the data subject being taken solely by a computer or other automated process.

14. Data security

14.1. The Trust will ensure that appropriate measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Appropriate measures include:

14.1.1. USB Pen drives/ "Sticks" are not permitted – unless specially encrypted and password protected external devices authorised for use by CEO, MAT Data Protection Officer or Academy Principal.

14.1.2. Network policies have been amended to prevent the use of USB Pen Drives (unless device is authorised as above)

14.2. Appropriate levels of authority being given to staff members where access to personal data is concerned;

14.2.1. Keeping the data in a locked filing cabinet, drawer or safe;

14.2.2. Ensuring that computerised data is coded, encrypted or password protected, both on the local hard drive of laptops~~;~~

14.2.3. Network drives are regularly backed up off site;

14.2.4. Where data is saved on removable storage, holding the storage device in a locked filing cabinet, drawer or safe.

14.3. The Trust has in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. The Trust will only transfer personal data to a third party if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

14.4. The Trust will have in place a written contract with each data processor (as defined by Section 1 of the DPA) used to carry out tasks for the Trust Board that necessitates the data processor having access to personal data processed by the Trust.

14.5. Maintaining data security means guaranteeing the confidentiality, integrity and availability (for authorised purposes) of the personal data.

14.6. In the event of a data breach, staff must report the incident to the MAT Data Protection Officer. Failure to do so may result in disciplinary action being taken. If staff are unsure as to whether an incident constitutes a data breach, they should report it.

15. Providing information to third parties

15.1. The Trust will not disclose personal data to a third party without the data subject's consent unless the Trust is satisfied that they are legally entitled to the data. Where the Trust does disclose personal data to a third party, the Trust will have regard to the eight data protection principles.

15.2. If staff receive a request from a third party for personal data, or consider that they need to disclose personal data to a third party, they should seek advice from the MAT Data Protection Officer. This may include (but is not limited to) requests from parents, or other members of staff, for personal data relating to other members of staff (including temporary staff), agency workers, volunteers, suppliers, pupils, their parents, guardians or carers, and other individuals (including suppliers and governors).

15.3. Any member of staff who knowingly or recklessly, without the Trust Board's consent, obtains or discloses personal data or procures the disclosure to another person, commits an offence under Section 55 of the DPA and may be subject to disciplinary proceedings under the Trust Board's Disciplinary Policy.

16. Subject access requests under the DPA

16.1. If a data subject wishes to know what personal data the Trust holds about him/her, he/she must make the request in writing, with an accompanying fee of £10. All such written requests should be forwarded to the MAT Director of Operations.

16.2. The Trust Board will have 40 calendar days to respond to a valid subject access request**.**

16.3. Any member of staff that receives a subject access request (or believes that they may have done so) should forward it without delay to the MAT Data Protection Officer. The Trust Board has a statutory timeframe to adhere to which is 40 calendar days, and failure to promptly report a subject access request (or a request believed to be a subject access request) may lead to disciplinary action.

17. Breaches of data protection

17.1. If a data subject considers that this policy has not been followed in respect of personal data about a data subject he/she should raise the matter with the MAT Data Protection Officer.

17.2. Any breach of this policy by staff will be taken seriously and may result in disciplinary action.

FREEDOM OF INFORMATION

18. Publication scheme

18.1. The Trust Board understands its duties under the FOIA to be transparent and proactive in relation to the information that it makes public.

18.2. The Trust Board has adopted the ICO's Model Publication Scheme and this is available on the Trust's website.

19. Requests

19.1. The FOIA applies to all recorded information held by the Trust Board, along with information held by a third party organisation on behalf of the Trust Board.

19.2. Any member of staff that receives a freedom of information request (or believes that they may have done so) should forward it without delay to the Director of Operations. The Trust Board has a statutory timeframe to adhere to which is 20 working days, and failure to promptly report a freedom of information request (or a request believed to be a freedom of information request) may lead to disciplinary action.

19.3. The Trust Board will provide a response to a freedom of information request within 20 working days unless the data subject is notified that the statutory timeframe is extended by a necessity to consider the public interest test.

20. **Advice and assistance**

20.1. The Trust Board will provide advice and assistance to requesters in accordance with Section 16 of the FOIA**.**

21. **Internal review**

21.1. The Trust Board operates an internal review procedure for any requester that is dissatisfied with the handling of their freedom of information request by the Trust. Internal reviews will be carried out by a senior member of staff who has not been involved in making the original decision or responding to the request.

21.2. As part of the Trust's internal review procedure, the Trust Board will consider whether or not the request was handled appropriately and in accordance with the requirements of the FOIA.

21.3. Requesters seeking an internal review must write to the MAT Data Protection Officer within 40 working days of the date of the Trust's response to the original request stating the grounds for the review.

21.4. The Trust will endeavour to respond to requests for internal review within 20 calendar days of receipt of the request. Where this is not possible, the Trust will write to the requester to inform them of the expected date of response to their request for internal review.

21.5. Requesters who are unhappy with the outcome of the internal review may raise a complaint with the ICO.