Diocese of Bristol Academies Trust

Data Protection Policy

Easton CE Academy

Date Adopted: 4th June 2015

Review Date:

History of most recent Policy changes (must be completed)

Date	Page	Change	Origin of Change e.g. TU request, Change in legislation

Contents

1) Preamble 4
2) Overriding principles 4
3) About this policy 4
4) Definition of data protection terms 5
5) Data protection principles 5
6) Fair and lawful processing 5
7) Processing for limited purposes 6
8) Adequate, relevant and non-excessive processing 6
9) Accurate data 6
10) Data retention 7
11) Processing in line with data subjects' rights 7
12) Data security 7
13) Security procedures include: 7
14) Subject access requests 8
15) Providing information to third parties 8
16) Complaints 8
Appendix 1: Procedure for Subject Access Requests 9
1) Making a subject access request 9
2) Responding to a subject access request 9
3) Circumstances where we may refuse a subject access request 10
Appendix 2: Draft letters relating to subject access requests 11
Acknowledgment of data subject access request 11
Letter seeking fee, identification or clarification 11
Response to subject access request 12

1) Preamble

a) The Trust is an organisation with a Christian foundation. The ethos, values and relationships of the Trust, and its associated academies, are central to witnessing to the value of the foundation. The Trust aims to protect the privacy of all staff and pupils/students when processing and storing data and in accordance with the Data Protection Act.

b) The Diocese of Bristol Academies Trust (DBAT) has a legal duty to ensure that its academies process personal information in a way which is compliant with the Data Protection Act 1998. The Main Board of DBAT has delegated this responsibility to the Academy.

c) The Academy has adopted this policy to set out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information held by the Academy.

2) Overriding principles

a) Everyone has rights with regard to how their personal information is handled. During the course of our activities, the Academy will collect, store and process personal information about our staff, pupils and parents/carers of pupils, suppliers and other third parties. We recognise the need to treat such information in an appropriate and lawful manner.

b) We have a duty to be registered as a data controller with the Information Commissioner's Office (ICO) detailing the information held and its use. Details are available on the ICO's website.

3) About this policy

a) The types of information that we may be required to handle include details of current, past and prospective employees, pupils and parents/carers of pupils, suppliers and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 ("**DPA**") and other regulations. The DPA imposes restrictions on how we may use that information.

b) This policy has been approved by the Local Board of Easton CE Academy. It sets out our rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

c) All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to this policy.

4) Definition of data protection terms

"Data" is information which is stored electronically, on a computer, or in paper-based filing systems.

"Data controllers" are organisations which determine how personal data is processed. We are the data controller of all personal data used in our Academy.

"Data subjects" for the purpose of this policy includes all living individuals about whom we hold personal data.

"Data users" include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection policy at all times.

"Data processors" include any person who processes personal data on behalf of a data controller e.g. suppliers.

"Personal data" means data relating to a living individual who can be identified from that data. Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance management appraisal).

"Processing" is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it or transferring personal data to third parties.

"Sensitive personal data" includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

5) Data protection principles

a) Anyone processing personal data must comply with the eight enforceable principles of good practice.

b) These provide that personal data must be:

i) Processed fairly and lawfully;
ii) Obtained only for one or more specified and lawful purpose, and shall not be processed in any manner incompatible with those purpose;
iii) Adequate, relevant and not excessive for the purpose;
iv) Accurate and kept up to date;
v) Not kept longer than necessary for the purpose;
vi) Processed in line with data subjects' rights;
vii) Kept secure;
viii) Not transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

6) Fair and lawful processing

a) The DPA is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case, the Academy), the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

b) For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for our legitimate interest.

c) When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

d) Data about staff may be processed for legal, personnel, administrative and management purposes and to enable us to meet our legal obligations, for example to pay staff, monitor their performance and to confer benefits in connection with their employment. Examples of when sensitive personal data of staff is likely to be processed are set out below:

- information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;
- an employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- in order to comply with legal requirements and obligations to third parties.

e) Data about pupils and parents/carers of pupils may be processed in order to enable us to provide education and other associated functions. In addition, there may be a legal requirement to collect and use information to ensure that we comply with our statutory obligations.

7) Processing for limited purposes

a) Personal data will only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the DPA. This means that personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

8) Adequate, relevant and non-excessive processing

a) Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose will not be collected in the first place.

9) Accurate data

a) Personal data will be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

10) Data retention

a) Personal data will not be kept longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required.

11) Processing in line with data subjects' rights

a) Data will be processed in line with data subjects' rights. Data subjects have a right to:

i) Request access to any data held about them us;
ii) Prevent the processing of their data for direct-marketing purposes;
iii) Ask to have inaccurate data amended;
iv) Prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else;
v) Object to any decision that significantly affects them being taken solely by a computer or other automated process.

12) Data security

a) We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

b) The DPA requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

c) Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who are authorised to use the data can access it;
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed;
- Availability means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

13) Security procedures include:

- Entry controls - any stranger seen in entry-controlled areas should be reported;

- Secure lockable desks and cupboards - desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential);
- Methods of disposal - paper documents should be shredded and floppy disks and CD-ROMs should be physically destroyed when they are no longer required;
- Equipment - data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

14) Subject access requests

a) Our procedures for responding to formal requests from a data subject for information that we hold about them is set out in Appendix 1. We reserve the right to charge up to £10 to provide the information requested.

15) Providing information to third parties

a) Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us.

b) In particular they should:

- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested;
- Suggest that the third party put their request in writing so the third party's identity and entitlement to the information may be verified;
- Refer to the Principal for assistance in difficult situations;
- Where providing information to a third party, do so in accordance with the eight data protection principles.

16) Complaints

a) Complaints will be dealt with in accordance with the Academy's complaints policy. Complaints relating to information handling may be referred to the Information Commissioner.

APPENDIX 1: PROCEDURE FOR SUBJECT ACCESS REQUESTS

1) Making a subject access request

a) An individual is only entitled to access their own personal data, and not to information relating to other people. Individuals with parental responsibility may make requests for personal information relating to their child, unless we determine that the child has the capacity to make their own decisions about their personal information. In these circumstances, we will discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their personal data.

b) For a subject access request to be valid, it must be made in writing e.g. letter, email or fax. It is helpful if the person requesting the information identifies the request as a subject access request and addresses the request to the Principal.

c) The request must be sufficiently detailed to enable us to identify and find the personal data covered by the request. If we are unsure, we can request further information. Until this further information is received, we do not need to comply with the subject access request.

d) The request must also be accompanied by a cheque for £10 made payable to the Academy. We do not need to comply with the subject access request until we have received this fee.

e) We are also entitled to request information to judge whether the person making the request is the individual to whom the personal data relates and/or is a person with parental responsibility for a child whose data is the subject of the request. This is to avoid personal data about one individual being sent to another, accidentally or as a result of deception.

f) Evidence of identity may be established by production of:
    - passport
    - driving licence
    - utility bills with the current address
    - birth / marriage certificate
    - P45/P60
    - credit card or mortgage statement

2) Responding to a subject access request

a) The response time for subject access requests, once officially received, is 40 calendar days (irrespective of school holidays). However, as set out above, the 40 calendar days will not commence until after receipt of the required fee, evidence of identity or clarification of information sought.

b) When responding to a subject access request, we will:

i) acknowledge receipt of your request and provide an indication of the likely timescale for a response within 5 working days;
ii) take all reasonable and proportionate steps to identify and disclose the data relating to the request;
iii) never delete information relating to a subject access request, unless it would have been deleted in the ordinary course of events;
iv) consider whether to seek consent from any third parties which might be identifiable from the data being disclosed;
v) seek legal advice, where necessary, to determine whether we are required to comply with the request or supply the information sought;
vi) provide a written response, including an explanation of the types of data provided and whether and for what reasons any data has been withheld;
vii) ensure that information disclosed is clear and technical terms are clarified and explained.

3) Circumstances where we may refuse a subject access request

a) We are not required to comply with a subject access request in relation to:

i) confidential references given by us for employment or educational purposes;
ii) personal data processed in connection with management forecasting or planning if it would prejudice the conduct of the business of the Academy;
iii) personal data subject to legal professional privilege;
iv) information which may cause serious harm to the physical or mental health or emotional condition of a child or another, or which would reveal that a child is at risk of abuse, or information relating to court proceedings.

b) We are also not required to supply the information requested if:

i) the data requested is not available;
ii) it would involve disproportionate effort to disclose the information requested;
iii) an identical or similar request has been made by the same individual previously, unless a reasonable interval has elapsed between the previous and the current request; in determining whether a 'reasonable interval' has elapsed, we will have regard to the nature of the data, the purpose for which the data is processed and the frequency with which the data is altered;
iv) we cannot comply with the request without disclosing information relating to another individual who can be identified from that information, unless:
- the other individual has consented to the disclosure of the information, or .
- it is reasonable in all the circumstances to comply with the request without the consent of the other individual; in determining whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned, we shall have regard shall be had to any duty of confidentiality owed to the other individual and any express refusal of consent by the other individual.

c) In order to provide the whole or some of the information requested, we may undertake redaction (information blacked out/removed) of one or more documents. An explanation of why we have redacted the information will be provided.

APPENDIX 2: DRAFT LETTERS RELATING TO SUBJECT ACCESS REQUESTS

Acknowledgment of data subject access request

Dear [NAME],

I write to acknowledge receipt of your [data subject access request under section 7 of the Data Protection Act 1998] OR [request for personal information which we are responding to under section 7 of the Data Protection Act 1998.]

I also acknowledge receipt of your cheque for £10 together with a copy of your [INSERT IDENTIFICATION PROVIDED] as confirmation of your identity.

Your request was received on [DATE] and, unless there are grounds for extending the statutory deadline of 40 calendar days, we expect to be able to give you a response by [DATE].

Yours sincerely.

Letter seeking fee, identification or clarification

Dear [NAME],

So that we may process your request, I would be grateful if you could provide confirmation of your identity in the form of [IDENTIFICATION REQUIRED]. We will also require payment of the fee of £10 before we are able to process the request. Please provide a cheque made payable to [INSERT].

In addition, please provide us with further information about the information you want. Fr example, please include time frames, dates, names or types of documents, any file reference and any other information that may enable us to locate the personal data you seek.

Please note that under the Data Protection Act 1998 we are not obliged to supply the information requested until we receive the information requested above. The deadline of 40 calendar days in which to respond to your request will start to run as soon as we receive it.

Yours sincerely,

Response to subject access request

Dear [NAME],

We write further to your request for details of personal data which we hold [and our acknowledgment of [DATE WHEN REQUEST FIRST ACKNOWLEDGED BY LETTER]].

We enclose data in the following format:

[DETAILS OF FORMAT IN WHICH DATA IS PROVIDED, WITH REASONS FOR CHOOSING THE FORMAT: PAPER COPIES OR ELECTRONIC COPIES ON A CD OR FLOPPY DISC OR A NEW DOCUMENT WHICH HAS BEEN CREATED AND WHICH SETS OUT THE INFORMATION WHICH CONSTITUTES PERSONAL DATA]

Some names and identifying particulars have been deleted to protect the identity of third parties.

Some personal data has been omitted because:

- [It consisted of a confidential reference given by us for employment purposes.]
- [It consisted of personal data processed in connection with management forecasting or planning, disclosure of which we considered would prejudice the conduct of the business of the Academy.]
- [It is subject to legal privilege.]
- [It consisted of records which we considered that disclosure of would be likely to cause serious harm to your physical or mental health or that of another person.]

Yours sincerely