BDMAT
Birmingham Diocesan
Multi-Academy Trust

General Data Protection Regulations Policy

Issued: October 2018
Next review due: Autumn 2020

General Data Protection Regulation (GDPR) Policy

1.0 Aims

1.1 The Birmingham Diocesan Multi-Academy Trust (BDMAT) aims to ensure that all data collected about staff, pupils, parents and visitors is collected, stored and processed in accordance with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR). This policy applies to all data, regardless of whether it is in paper or electronic format.

2.0 Legislation and guidance

2.1 This policy meets the requirement of the Data Protection Act 1998 and is based on guidance published by the Information Commissioner's Office and model privacy notices published by the Department of Education.

2.2 It also takes into account the expected provisions of the General Data Protection Regulations, which is new legislation due to come into force on 25 May 2018.

2.3 In addition, this policy complies with regulation 5 of the Education (Pupil information) (England) Regulations 2005, which gives parents the right of access to their child's educational record.

2.4 This policy complies with our funding agreement and articles of association.

3.0 Definitions

Term	Definition
Personal data	Data from which a person can be identified, including data that, when combined with other readily available information, leads to a person being identified.
Sensitive data	Data such as: • Contact details • Racial or ethnic origin • Political opinions • Religious beliefs, or beliefs of a similar nature

	• Where a person is a member of a trade union • Physical and mental health • Sexual orientation • Whether a person has committed, or is alleged to have committed, an offence • Criminal convictions • Biometrics
Processing	Obtaining, recording or holding data
Data Subject	The person for whom personal data is held or processed
Chief Privacy Officer	A person or organisation that determines the purpose for which, and the manner in which, personal data is processed
Data processor	A person, other than an employee of the data controller, who processes the data on behalf of the data controller

4.0 Chief Privacy Officer

4.1 BDMAT processes personal information relating to the pupils, staff and visitors, and therefore, is a data controller. BDMAT Board of Directors delegates the responsibility of data controller to the Finance Director.

4.2 BDMAT is registered as a data controller with the Information Commissioner's Office and renews this registration annually.

5.0 Data protection principles

5.1 The Data Protection Act 1998 is based on the following data protection principles, or rules for good data handling:

- Data shall be processed fairly and lawfully;
- Personal data shall be obtained only for one or more specified and lawful purposes;
- Personal data shall be relevant and not excessive in relation to the purpose(s) for which it is processed;
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998;

- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of, or damage to, personal data;
- Personal data shall not be transferred to a country or territory outside the European Economic Area unless the country or territory ensures an adequate level of protection for the rights and freedoms of data in relation to the processing of personal data.

6.0 Roles and responsibilities

6.1 The BDMAT Board has overall responsibility for ensuring that BDMAT complies with its obligations under the Data Protection Act 1998.

6.2 Day-to-day responsibilities rest with the Headteacher and the Local Academy Board (LAB).

6.2 The Headteacher will ensure that all staff are aware of their data protection obligations, and oversee any queries related to the storing or processing of personal data.

6.3 Staff are responsible for ensuring that they collect and store any personal data in accordance with this policy. Staff must also inform the school of any changes to their personal data, such as a change of address.

7.0 Privacy/fair processing notice

7.1 Pupil and parents

7.11 We hold personal data about pupils to support teaching and learning, to provide pastoral care and to assess how the school is performing. We may also receive data about pupils from other organisations including, but not limited to, other schools, local authorities and the Department for Education.

7.12 This data includes, but is not restricted to:

- Contact details;
- Results of internal assessment and externally set tests;
- Data on pupil characteristics, such as ethnic group or special educational needs;
- Exclusion information;
- Details of any medical conditions.

7.13 We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

7.14 We will not share information about pupils with anyone without consent unless the law and our policies allow us to do so. Individuals who wish to receive a copy of the information that we hold about them/their child should refer to sections 8 and 9 of this policy.

7.15 We are required, by law, to pass certain information about pupils to specified external bodies, such as local authorities and the Department of Education, so that they are able to meet their statutory obligations.

7.2 Staff

7.21 We process data relating to those we employ to work at, or otherwise engage to work at, our schools. The purpose of processing this data is to assist in the school, including to:

- Enable individuals to be paid;
- Facilitate safe recruitment;
- Support the effective performance management of staff;
- Improve the management of workforce data across the sector;
- Inform our recruitment and retention policies;
- Allow better financial modelling and planning;
- Enable ethnicity and disability monitoring.

7.22 Staff personal data includes, but is not limited to, information such as:

- Contact details;
- National Insurance numbers;
- Salary information;
- Qualifications;
- Absence data;
- Personal characteristics, including ethnic groups;
- Medical information;
- Outcomes of any disciplinary procedures.

7.23 We will only retain the data we collect for as long as is necessary to satisfy the purpose for which it has been collected.

7.24 We will not share information about staff with third parties without consent unless the law allows us to.

7.25 We are required, by law, to pass certain information about staff to specified external bodies, such as local authorities and the Department of Education, so that they are able to meet their statutory obligations.

7.26 Any staff members wishing to see a copy of information about them that BDMAT holds should contact the relevant establishment lead or Headteacher/Finance Director.

8.0 Subject access requests

8.1 Under the General Data Protection Act 2018, pupils have a right to request access to information the school holds about them. This is known as a subject access request.

8.2 Subject access requests must be submitted in writing, either by letter, email or fax. Requests should include:

- The pupil's name;
- A correspondence address;
- A contact number and email address;
- Details about the information requested.

8.3 The school will not reveal the following information in response to subject access requests:

- Information that might cause serious harm to the physical or mental health of the pupil or another individual;
- Information that would reveal that the child is at risk of abuse, where disclosure of that information would not be in the child's best interest;
- Information contained in adoption and parental order records;
- Certain information given to a court in proceeding concerning the child.

8.4 Subject access request for all or part of the pupil's educational record will be provided within 31 days.

9.0 Parental requests to see the education record

9.1 Parent have the right of access to their child's educational record, free of charge, within 15 school days of a request.

9.2 Personal data about a child belongs to that child, and not the child's parents. This is the case even where a child is too young to understand the implications of subject access right.

9.3 For a parent to make a subject access request, the child must either be unable to understand their rights and implications of a subject access request or have given their consent.

9.4 The Information Commissioner's Office, the organisation that upholds information rights, generally regards children aged 12 above as mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents of pupils at schools within BDMAT may be granted without the express permission of the pupil.

9.5 Parents of pupils at schools within BDMAT do not have an automatic right to access their child's educational record. The school will decide on a case-by-case basis whether to grant such request, and we will bear in mind guidance issued from time to time from the Information Commissioner's Officer (the organisation that upholds information rights).

10.0 **Storage of records**

10.1 Paper-based records and portable electronic devices, such as laptops and hard drives, that contain personal information are kept under lock and key when not in use.

10.2 Papers containing confidential personal information should not be left on office and classroom desks, on staffroom tables or pinned to noticeboards where there is general access, unless there is a clear medical reason and that there is explicit written consent i.e. allergy advice in school kitchens.

10.3 Where personal information needs to be taken off site (in paper or electronic form), staff must sign it in and out from the school office.

10.4 The Headteacher may authorise staff to use school laptops off site.

10.5 Passwords that are at least 8 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices.

10.6 Staff and pupils are reminded to change their password at regular intervals.

10.7 Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures for school-owned equipment.

BDMAT
Birmingham Diocesan Multi-Academy Trust

11.0 Disposal of records

11.1 Personal information that is no longer needed or has become inaccurate, or out of date, is disposed of securely.

11.2 For example, we will shred or incinerate paper-based records and override electronic files. We may also use an outside company to safely dispose of electronic records.

12.0 Training

12.1 Our staff and governors including Directors will be provided with data protection training as part of their induction process.

12.2 Data protection will also form part of continuing professional development, where changes to legislation or the school's processes make it necessary.

13.0 Withdrawing Consent

13.1 Consent can be withdrawn subject to contractual, statutory or regulatory constraints. Where more than one person has the ability to provide or withdraw consent BDMAT will consider each situation on its merits and within the principles of GDPR and also child welfare, protection and safeguarding principles. We have provided a form for you to withdraw consent and this is in Appendix 1.

14.0 Complaints

14.1 If you have a concern about how your data has been collected, used, held or processed by BDMAT then please refer to BDMAT's Complaints Procedure in the first instance which is available on our website. You have a right to complain if you feel that data has been shared without consent or lawful authority, or if you have asked us to erase, rectify, not process data and we have not agreed to your request. We will seek to resolve issues on an informal basis and then through our formal complaints procedure.

14.2 In the UK it is the ICO who has responsibility for enforcing the GDPR obligations and their contact details can be found at www.ico.org.uk Helpline: 0303 123 1113 Email: casework@ico.org.uk

15.0 Monitoring arrangements

15.1 The Finance Director is responsible for monitoring and reviewing this policy.

15.2 The Headteacher alongside the Local Academy Board checks that the school complies with this policy by, among other things, reviewing school records termly.

15.3 This document will be reviewed every 2 years.

Appendix 1a

Birmingham Diocesan Multi-Academy Trust

Withdrawal of Consent Form – on behalf of pupil

Please complete and sign this form and deliver it to the school office.

Please note that as a Trust we may have contractual, statutory and/or regulatory reasons why we will still process and hold details of a pupil, parent, staff member, volunteer or other person.

Where there is shared parental responsibility or where the pupil is capable of expressing a view and there is conflict between the individuals; the process of withdrawing consent will be subject to an evaluation and discussion. This is to enable a decision to be reached that is considered to be in the pupil's best interest.

We may need to seek identification evidence and have sight of any Court Order or Parental Responsibility Agreement in some cases to action this request. If this is the case, a senior member of the school staff will discuss this with you.

I withdraw consent for BDMAT to process the personal data described below relating to the name pupil.

Name of person withdrawing consent	
Name of pupil that this withdrawal concerns	
A description of the personal data that this withdrawal concerns and for which consent was previously granted	
I confirm that I am the parent or carer of the named pupil and that I have parental responsibility for the pupil	*Signed:* *Date:*

For BDMAT use only:	
Date received by BDMAT	
Name of staff member receiving withdrawal of consent form	
Record of actions taken	

Appendix 1b

Birmingham Diocesan Multi-Academy Trust

Withdrawal of Consent Form – Adult

Please complete and sign this form and deliver it to school office.

Please note that as a Trust we may have contractual, statutory and/or regulatory reasons why will still process and hold details of a pupil, parent, staff member, volunteer or other person.

I withdraw consent for BDMAT to process the personal data described below for which consent was previously granted.

Name of person withdrawing consent	
A description of the personal data that this withdrawal concerns and for which consent was previously granted	
Signed: *Date:*	

For BDMAT use only:	
Date received by BDMAT	
Name of staff member receiving withdraw form	
Record of actions taken	

Appendix 2

Birmingham Diocesan Multi-Academy Trust

Procedures for responding to Subject Access Requests made under the Data Protection Act 2018 and General Data Protection Regulation

Rights of access to information

There are two distinct rights of access to information held by schools about individuals:

1. Under the Data Protection Act 2018 and GDPR any individual has the right to make a request to access the personal information held about them.
2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (England) Regulations 2005.

Actioning a subject access request

1. Request for information must be made in writing and we have provided a form for this purpose: "Subject Access Request Form" which can be sent by email addressed to the Data Protection Officer. If the initial request does not clearly identify the information required, then further enquiries will be made to establish the information required.
2. The identity of the requestor must be established before the disclosure of any information, and checks will be carried out regarding proof of relationship to the child if a request is being made by a parent. Evidence of identity can be established by a combination of the following documents:
    - passport
    - driving licence
    - utility bills with current address
    - birth/marriage certificate
    - P45/P60
    - Credit card or mortgage statement

    This is not an exhaustive list – please see Subject Access Request Form
3. Any individual has the right of access to information held about themselves. However, with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. Personal data about a

child belongs to that child. The Trust will decide on a case by case basis whether to grant such request, bearing in mind guidance issued from time to time from the Information Commissioner's Office.

4. The response time for subject access requests for all or part of the pupil's educational record, once officially received, is 15 school days. If the subject access request does not relate to the educational record, we will respond within one month. However, the one month will not commence until after clarification of the information sought.
5. The Data Protection Act 2018 allows exemptions regarding the provision of some information: therefore, all information will be reviewed prior to disclosure.
6. Third party information is that which has been provided by another body, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent will normally be obtained. The 40 statutory timescales will still apply.
7. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another individual may not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings be disclosed.
8. If there are concerns over the disclosure of information, then additional advice should be sought.
9. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.
10. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.
11. Information can be provided at the school with a member of staff on hand to help and explain matters if requested. The view of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used, then registered/recorded mail must be used.

Safeguarding

BDMAT's responsibilities in relation to Child Protection and Safeguarding will always be considered and where there is any doubt about whether or not to disclose information then Safeguarding priorities will take precedence over data protection and subject access requests.

Complaints

Complaints about the above procedures should be referred to BDMAT's Finance Director who will decide whether it is appropriate for the complaint to dealt with in accordance with BDMAT's Complaints Policy. Complaints which are considered to be outside the scope of BDMAT's Complaints Policy can be dealt with by the Information Commissioner. Contact details of both will be provided with the disclosure information.

Contacts

If you have any queries or concerns regarding this procedure, then please contact the Data Protection Officer. Contact details are available on request.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone 0303 123 1113.

Birmingham Diocesan Multi-Academy Trust

SUBJECT ACCESS REQUEST FORM

Please complete this form if you want us to supply you with a copy of any personal data we hold about you. You are entitled to receive this information under the Data Protection Act 2018 (DPA) and the EU General Data Protection Regulation (GDPR), which comes into effect on 25 May 2018. We will also provide you with information about any processing of your personal data that is being carried out, the retention periods which apply to your personal data, and any rights to rectification, erasure, or restriction of processing that may exist.

We will endeavour to respond promptly and in any event within one month of the latest of the following:

- Our receipt of your written request; or
- Our receipt of any further information we may ask you to provide to enable us to comply with your request.

The information you supply in this form will only be used for the purposes of identifying the personal data you are requesting and responding to your request. You are not obliged to complete this form to make a request but doing so will make it easier for use to process your request quickly.

1) **Details of the person requesting information**

Full Name:

Address (including postcode):

Contact Telephone Number:

Contact Email Address:

To ensure we are releasing data to the right person we require you to provide us with proof of your identity and of your address. If we are not satisfied you are who you claim to be, we reserve the right to refuse to grant your request.

Please supply us with a photocopy or scanned image (do not send the originals) of one of **both** of the following:

a) Proof of Identity Passport, photo driving licence, national identity card, birth certificate.
b) Proof of Address Utility bill, bank statement, credit card statement (no more than 3 months old); current driving licence; current TV licence; local authority tax till, HMRC tax document (no more than 1 year old). Alternatively, you can post this proof of identification to BDMAT.

2) What information are you seeking?

Please describe the information you are seeking. Please provide any relevant details you think will help us to identify the information you require. Please note that if the information you request reveals details directly or indirectly about another person we will have to seek the consent of that person before we can let you see that information. In certain circumstances, where disclosure would adversely affect the rights and freedoms of others, we may not be able to disclose the information to you, in which case you will be informed promptly and given full reasons for that decision. While in most cases we will be happy to provide you with copies of the information you request, we nevertheless reserve the right, in accordance with Article 12 of the GDPR to charge a fee or refuse the request if it is considered to be "manifestly unfounded or excessive". However, we will make every effort to provide you with a satisfactory form of access or summary of information if suitable.

3) Information about the collection and processing of data

If you want information about any of the following, please tick the boxes:

☐ Why we are processing your personal data

☐ To whom your personal data is disclosed

☐ The source of your personal data

BDMAT
Birmingham Diocesan
Multi-Academy Trust

4) Declaration

I confirm that I have read and understood the terms of this subject access form and certify that the information given in this application is true. I understand that it is necessary for BDMAT to verify my identity and it may be necessary to obtain more detailed information in order to locate the correct personal data.

Signed: Date:

Appendix 3

Birmingham Diocesan Multi-Academy Trust

Data Breach Procedures

This procedure is designed to ensure that all staff, governors and directors are aware of what to do in the event of DPA/GDPR breach and that they need to act swiftly to report the breach.

BDMAT's recognises that most breaches, aside from cyber criminal attacks, occur as a result of human error. They are not malicious in origin and if quickly reported are often manageable.

Examples of breaches are:-

- Information being posted to an incorrect address which results in an unintended recipient reading that information
- Loss of mobile or portable data device, unencrypted mobile phone, laptop, USB memory stick or similar
- Sending an email with personal data to the wrong person or to too many people who may not need to or be entitled to see the data
- Dropping or leaving documents containing personal data in a public place.
- Personal data being left unattended at a printer enable unauthorised personal to read that information
- Not securing documents containing personal data (at home or work) when left unattended
- Anything that enables an unauthorised individual access to school buildings or computer systems
- Discussing personal data with someone not entitled to it, either or phone or in person. How can you be sure they are entitled to that information?
- Deliberately accessing or attempting to access or use personal data beyond the requirements of an individual's job role e.g. for personal, commercial or political use. This action may constitute a criminal offence under the Computer Misuse Act as well as the Data Protection Act.
- Opening a malicious email attachment or clicking on a link from external or unfamiliar source, which leads to BDMAT's equipment (and subsequently its records) being subjected to a virus or malicious attack, which results in unauthorised access to, loss, destruction or damage to personal data.

What should staff do?

Being open about the possible breach and explaining what has been lost or potentially accessed is an important element of working with the ICO to mitigate the impact. Covering up a breach is never acceptable and may be a criminal, civil or disciplinary matter. Report the breach to the Data Champion and Data Protection Officer as soon as possible, this is essential.

What will happen next?

The breach notification form will be completed and the breach register updated. The breach report to the ICO will be submitted within 72 hours of the Data Champion becoming aware of the breach.

If the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach notification to those people will be done in a co-ordinated manner with support from the DPO.

Breach notification to data subject

For every breach BDMAT will consider notification to the data subject or subjects as part of the process. If the breach is likely to be high risk, they will be notified as soon as possible and kept informed of actions and outcomes.

The breach and process will be described in clear and plain language.

If the breach affects a high volume of data subjects and personal data records, the most effective form of notification will be used and discussed with the Data Champion with support from the Data Protection Officer.

Advice will be taken from the ICO about how to manage communication with data subjects if appropriate.

A post breach action plan will be put into place and reviewed.

Evidence Collection

It may be necessary to collect information about how an information security breach or unauthorised release of data occurred. This evidence gathering process may be used as part of an internal process (which can include disciplinary proceedings), it may be a source of information for the ICO and it could also be used within criminal or civil proceedings.

This process will be conducted by a suitable member of BDMAT, which may be or not be the Data Protection Officer but will be determine the best way to secure evidence.

Guidance may be required from an external legal provider and the police may be involved to determine the best way to secure evidence.

A record of what evidence has been gathered, stored and secured must be available as a separate log. Files and hardware must be securely stored.

Evidence Collection Log

Date	Evidence Description	Secure storage location & confirmed date	Trust Officer

Data Breach Notification Form

When did the breach occur (or become known)?	
Who was involved in BDMAT?	
Who was this reported to?	
Date and time it was reported	
Date and time DPO notified	
A description of the nature of the breach. This must include the type of information that was lost, e.g. name, address, medical information, NI number	
The categories of personal data affected – electronic, hard copy	
Approximate number of data subjects affected	
Approximate number of personal data records affected	
Name and contact details of the Data Protection Officer/GDPR Owner	
Consequences of the breach. What are the potential risks?	

Any measures taken to address the breach. What actions and timeline have been identified?	
Any information relating to the data breach.	