


General Data Protection Regulations Policy

Issued: June 2018
Reviewed: Autumn 2021
Next Review due: Autumn 2022



Contents

1	Aims	3
2	Legislation and guidance	3
3	Definitions	4
4	The data controller	5
5	Roles and responsibilities	5
6	Data protection principles	7
7	Collecting personal data	8
8	Sharing personal data	10
9	Subject access requests and other rights of individuals	11
10	Parental requests to see the educational record	14
11	CCTV	14
12	Photographs and videos	14
13	Data protection by design and default	16
14	Data security and storage of records	16
15	Disposal of records	17
16	Personal data breaches	17
17	Training	18
18	Monitoring arrangements	18
	Appendices	
1a	Withdrawal of consent by parent or child (form)	19
1b	Withdrawal of consent by adult (form)	21
2	Responding to a SAR	22
3	The Subject Access Request form (SAR)	24
4	Personal data breach procedure	27



General Data Protection Regulation (GDPR) Policy

1.0 Aims

- 1.1 The Birmingham Diocesan Multi-Academy Trust (BDMAT) aims to ensure that all personal data collected about staff, pupils, parents, and visitors is collected, stored and processed in accordance with UK data protection law

This policy applies to all personal 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:

UK General Data Protection Regulations (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by [The Data Protection, Privacy and Electronic Communications \(Amendments etc\) \(EU Exit\) Regulations 2020](#)

[Data Protection Act 2018 \(DPA 2018\)](#)

- 2.2 It is based on guidance published by the Information Commissioner’s Office (ICO) on the [GDPR](#).
- 2.3 It meets the requirements of the [Protection of Freedoms Act 2012](#) when referring to our use of biometric data.
- 2.4 It also reflects the ICO’s [code of practice](#) for the use of surveillance cameras and personal information.
- 2.5 This policy complies with our funding agreement and articles of association.

3.0 Definitions

Term	Definition
<p>Personal data</p>	<p>Any information relating to an identified, or identifiable, living individual.</p> <p>This may include the individual's:</p> <ul style="list-style-type: none"> • Name (including initials) • Identification number • Location data • Online identifier, such as a username <p>It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural, or social identity.</p>
<p>Special categories of personal data</p>	<p>Personal data, which is more sensitive and so needs more protection, including information about an individual's:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetics • Biometrics (such as fingerprints, retina, and iris patterns), where used for identification purposes • Health – physical or mental • Sex life or sexual orientation
<p>Processing</p>	<p>Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying.</p> <p>Processing can be automated or manual.</p>

Data Subject	The identified or identifiable individual whose personal data is held or processed.
Data Controller	A person or organisation that determines the purposes and the means of processing of personal data.
Data processor	A person or other body, other than an employee of the data controller, who processes the data on behalf of the data controller
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

4.0 The data controller

- 4.1 BDMAT processes personal information relating to the pupils, staff, and visitors, and therefore, is a data controller.
- 4.2 BDMAT is registered as a data controller with the Information Commissioner's Office and renews this registration annually and has paid its data protection fee to the ICO as legally required.

5.0 Roles and responsibilities

This policy applies to all staff employed by BDMAT, and to external organisations and individuals working on its behalf. Staff who do not comply with this policy may face disciplinary action.

5.1 The Trust Board

The BDMAT Board has overall responsibility for ensuring that BDMAT complies with all relevant data protection obligations

5.2 Data Protection Officer (DPO)

The data protection officer (DPO) is responsible for overseeing the implementation of this policy, monitoring our compliance with data protection law, and developing related policies and guidelines where applicable.



They will provide an annual report of their activities directly to the Trust Board and, where relevant, report to the board their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO.

In line with Article 39 of UK GDPR the DPO's tasks include:

- Informing and advising BDMAT and its employees about their obligations to comply with UK GDPR and other data protection laws;
- Monitoring compliance with UK GDPR and other data protection laws, and with the BDMAT data protection policies, including managing internal data protection activities, raising awareness of data protection issues, training staff, and conducting internal audits;
- Advising on, and monitoring data protection impact assessments;
- Co-operating with the ICO; and
- Being the first point of contact for the ICO and for individuals whose data is being processed.

Full details of the DPO's responsibilities are set out in their job description.

Our DPO is Michele Fullwood (Head of School Support) and is contactable via dpo@bdmatschools.com.

5.3 The Headteacher

Day-to-day responsibilities in schools rest with the Headteacher. Centrally the day-to-day responsibilities rest with the Heads of Departments and the Executive Team.

5.4 All Staff

Staff are responsible for:

1. Ensuring that they collect, store, and process any personal data in accordance with this policy.
2. Informing the school of any changes to their personal data, such as a change of address.
3. Contacting the DPO (dpo@bdmatschools.com) in the following circumstances:

- With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure;
- If they have any concerns that this policy is not being followed;
- If they are unsure whether or not they have a lawful basis to use personal data in a particular way;
- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the UK;
- If there has been a data breach or they suspect, there may have been;
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals, including the storing or transfer of data; and
- Setting up any contracts or sharing personal data with third parties.

6.0 Data protection principles

6.1 The UK GDPR is based on the following data protection principles, that all our schools and central team must comply with:

- Data shall be processed fairly and lawfully and in a transparent manner.
- Personal data shall be collected for specified, explicit and legitimate purposes.
- Personal data shall be adequate, relevant, and limited to what is necessary to fulfil the purpose(s) for which it is processed.
- Personal data must be accurate and where necessary kept up to date.
- Personal data must be kept for no longer than is necessary for the purposes for which it was processed.
- Personal data must be processed in a way that ensures it is appropriately secure.
- 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; and
- 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.

6.2 This policy sets out how the MAT aims to comply with these principles.

7.0 Collecting personal data

7.1 Lawfulness, fairness, and transparency

We will only process personal data where we have one of 6 'lawful bases' (legal reasons) to do so under data protection law:

1. The data needs to be processed so that the school can fulfil a contract with the individual, or the individual has asked the school to take specific steps before entering into a contract.
2. The data needs to be processed so that the school can comply with a legal obligation.
3. The data needs to be processed to ensure the vital interests of the individual or another person i.e., to protect someone's life.
4. The data needs to be processed so that the school, as a public authority, can perform a task in the public interest or exercise its official authority.
5. The data needs to be processed for the legitimate interests of the school (where the processing is not for any tasks the school performs as a public authority) or a third party, provided the individual's rights and freedoms are not overridden.
6. The individual (or their parent/carer when appropriate in the case of a pupil) has freely given clear consent.

For special categories of personal data, we will also meet one of the special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a pupil) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims

- The data needs to be processed for reasons of substantial public interest as defined in legislation
- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest
- For criminal offence data, we will meet both a lawful basis and a condition set out under data protection law. Conditions include:
 - The individual (or their parent/carer when appropriate in the case of a pupil) has given consent
 - The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
 - The data has already been made manifestly public by the individual
 - The data needs to be processed for or in connection with legal proceedings, to obtain legal advice, or for the establishment, exercise, or defence of legal rights
 - The data needs to be processed for reasons of substantial public interest as defined in legislation

Whenever we first collect personal data directly from individuals, we will provide them with the relevant information required by data protection law.

We will always consider the fairness of our data processing. We will ensure we do not handle personal data in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

7.2 Limitation, minimisation, and accuracy

We will only collect personal data for specified explicit and legitimate reasons. We will explain these reasons to the individuals when we first collect their data.

If we want to use personal data for reasons other than those given when we first obtained it, we will inform the individuals concerned before we do so and seek consent where necessary.

Staff must only process personal data where it is necessary to do their jobs.

We will keep data accurate and, where necessary, up to date. Inaccurate data will be rectified or erased when appropriate.

In addition, when staff no longer need the personal data they hold, they must ensure it is deleted or anonymised. This will be done in accordance with the Trust's record retention schedule (see Retention Policy).

8.0 Sharing personal data

8.1 We will not normally share personal data with anyone else without consent, but there are certain circumstances where we may be required to do so. These include, but are not limited to, situations where:

- There is an issue with a pupil or parent/carer that puts the safety of our staff at risk;
- We need to liaise with other agencies – we will seek consent as necessary before doing this; and
- Our suppliers or contractors need data to enable us to provide services to our staff and pupils – for example, IT companies. When doing this, we will:
 - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with UK data protection law;
 - Establish a contract with the supplier or contractor to ensure the fair and lawful processing of any personal data we share; and
 - Only share data that the supplier or contractor needs to carry out their service.

8.2 We will also share personal data with law enforcement and government bodies where we are legally required to do so.

8.3 We may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of our pupils or staff.

8.4 Where we transfer personal data internationally, we will do so in accordance with UK data protection law

9.0 Subject access requests and other rights of individuals

9.1 Subject access requests:

Individuals have a right to make a “subject access request” to gain access to personal information that BDMAT holds about them. This includes:

- Confirmation that their personal data is being processed;
- Access to a copy of the data;
- The purposes of the data processing;
- The categories of personal data concerned;
- Who the data has been, or will be, shared with;
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period;
- Where relevant, the existence of the right to request rectification, erasure or restriction, or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- The source of the data, if not the individual;
- Whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual; and
- The safeguards provided if the data is being transferred internationally.

Subject access requests can be submitted in any form, but we may be able to respond more quickly if they are made in writing using the form located at [appendix 3](#) and include:

- Name of individual;
- A correspondence address;
- A contact number and email address; and
- Details about the information requested.

If staff receive a subject access request in any form, they must immediately forward it to the DPO.

9.2 Children and subject access requests:

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children below the age of 12 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our primary schools may be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Children aged 12 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, most subject access requests from parents or carers of pupils at our secondary school may not be granted without the express permission of the pupil. This is not a rule and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

9.3 Responding to subject access requests: [\(Please see Appendix 2 for further guidance\)](#)

1) When responding to requests we:

- May ask the individual to provide 2 forms of identification;
- May contact the individual via phone to confirm the request was made;
- Will respond without delay and within 1 month of receipt of the request (or receipt of the additional information needed to confirm identity where relevant);
- Will provide the information free of charge; and
- May tell the individual we will comply within 3 month of receipt of the request, where a request is complex or numerous. We will inform the individual of this within 1 month and explain why the extension is necessary.

2) We may not disclose information for a variety of reasons, such as if it is:

- 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 interests;
- Information that would include another person's personal data that we cannot reasonably anonymise, and we do not have the other person's consent and it would be unreasonable to proceed without it; and
- Part of certain sensitive documents, such as these related to a crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts.

3) If the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee to cover administrative costs. We will take into account whether the request is repetitive in nature when making this decision.

4) When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO or they can seek to enforce their subject access right through the courts.

9.4 Other data protection rights of the individual:

In addition to the right to make a subject access request (see above), and to receive information when we are collecting their data about how we use and process it (see section 7), individuals also have the right to:

- Withdraw their consent to processing at any time ([forms are in appendices 1a and 1b](#));
- Ask us to rectify, erase or restrict processing of their personal data (in certain circumstances);
- Prevent use of their personal data for direct marketing;
- Object to processing which has been justified on the basis of public interest, official authority, or legitimate interests;
- Challenge decisions based solely on automated decision making or profiling (i.e., making decisions or evaluating certain things about an individual based on their personal data with no human involvement);
- Be notified of a data breach (in certain circumstances);
- Make a complaint to the ICO; and

- Ask for their personal data to be transferred to a third party in a structured, commonly used, and machine-readable format (in certain circumstances).

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the DPO.

Our Data Protection Officer (DPO), is Michele Fullwood, Head of School Support, at 1 Colmore Row, Birmingham, B3 2BJ, dpo@bdmat.org.uk or 0121 426 0403

10.0 Parental requests to see the education record

- 10.1 Parents of pupils at schools within BDMAT do not have an automatic legal right to access their child's educational record. We will however, in good faith and in line with maintained schools; give parents, or those with parental responsibility, free access to their child's educational record (which includes most information about a pupil) within 15 school days of receipt of a written request.
- 10.2 There are certain circumstances in which these requests can be denied, such as if releasing the information might cause serious harm to the physical or mental health of the pupil or another individual, or if it would mean releasing exam marks before they are officially announced.

11.0 CCTV

We use CCTV in various locations around the school site to ensure it remains safe. We will adhere to the ICO's [code of practice](#) for the use of CCTV.

We do not need to ask individuals' permission to use CCTV, but we make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

Any enquiries about the CCTV system should be directed to the Headteacher.

12.0 Photographs and videos

As part of our school activities, we may take photographs and record images of individuals within our schools.

In our primary schools:

We will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials. We will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers have agreed to this.

In our secondary schools:

We will obtain written consent from parents/carers (for pupils under 18), or pupils aged 18 and over, for photographs and videos to be taken of pupils for communication, marketing, and promotional materials.

Where we need parental consent, we will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where we don't need parental consent, we will clearly explain to the pupil how the photograph and/or video will be used.

Any photographs and videos taken by parents/carers at school events for their own personal use are not covered by data protection legislation. However, we will ask that photos or videos with other pupils are not shared publicly on social media for safeguarding reasons, unless all the relevant parents/carers (or pupils where appropriate) have agreed to this.

All schools:

Where the school takes photographs and videos, uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc.;
- Outside of school by external agencies such as the school photographer, newspapers, campaigns; and
- Online on our school website or social media pages.

Consent can be refused or withdrawn at any time. If consent is withdrawn, we will delete the photograph or video and not distribute it further.

(Forms for withdrawing consent can be found at appendix 1a and 1b of this document)

When using photographs and videos in this way we will not accompany them with any other personal information about the child, to ensure they cannot be identified.

13.0 Data protection by design and default.

We will put measures in place to show that we have integrated data protection into all of our data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge;
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 6);
- Completing data protection impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process);
- Integrating data protection into internal documents including this policy, any related policies and privacy notices;
- Regularly training members of staff on data protection law, this policy, any related policies, and any other data protection matters; we will also keep a record of attendance;
- Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant;
- Appropriate safeguards being put in place if we transfer any personal data outside of the UK, where different data protection laws may apply; and
- Maintaining records of our processing activities, including:
 - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices);
 - For all personal data that we hold, maintaining an internal record of the type of data, type of data subject, how and why we are using the data, any third-party recipients, any transfers outside of the UK and the safeguards for those, retention periods and how we are keeping the data secure.

14.0 Data security and storage of records

We will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing, or disclosure, and against accidental or unlawful loss, destruction, or damage. In particular:

- Paper-based records and portable electronic devices that contain personal information are kept under lock and key when not in use;
- Papers containing confidential personal information must 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;
- The Headteacher may authorise staff to take or keep school laptops off site, if they are required to complete duties within their professional role;
- We recommend that passwords of at least -10 characters long containing letters and numbers are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded that they should not re-use passwords from other sites;
- The trust is working towards having encryption software installed to protect all portable devices and removable media, such as laptops and USB devices; and
- Where we need to share personal data with a third party, we carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 8).

15.0 Disposal of records

15.1 Personal information that is no longer needed will be disposed of securely. Personal data that has become inaccurate, or out of date, will also be disposed of securely, where we cannot or do not need to rectify or update it.

15.2 For example, we will shred or incinerate paper-based records and override or delete electronic files. We may also use third party to safely dispose of records on the Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

16.0 Personal data breaches

16.1 The Trust will make all reasonable endeavours to ensure that there are no personal data breaches.

16.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in [appendix 4](#).

16.3 When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it. Examples of such breaches in an education context could include:

- A non-anonymised dataset being published on the school website which shows the exam results of pupils eligible for the pupil premium;
- Safeguarding information being made available to an unauthorised person; and
- The theft of a school laptop containing non-encrypted personal data about pupils.

17.0 Training

- 17.1 Our staff and governors including Directors will be provided with data protection training as part of their induction process.
- 17.2 Data protection will also form part of continuing professional development.

18.0 Monitoring arrangements

- 18.1 The DPO is responsible for monitoring and reviewing this policy.
- 18.2 This policy will be reviewed annually and approved by the Trust Board in line with DfE recommendations on statutory policies

<https://www.gov.uk/government/publications/statutory-policies-for-schools-and-academy-trusts>

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	<i>Signed:</i> <i>Date:</i>



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	
<i>Signed:</i>	
<i>Date:</i>	

<i>For BDMAT use only:</i>	
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 UK General Data Protection Regulation (the EU GDPR was incorporated into UK legislation, with some amendment, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020

Rights of access to information

Under the Data Protection Act 2018 and the UK GDPR any individual has the right to make a request to access the personal information held about them. This is known as a subject access request or SAR.

Actioning a subject access request

1. Requests for information do not need be made in writing, however, to help in dealing with your request we have provided a form for this purpose: "Subject Access Request Form" (Appendix 3) 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 statutory timescale of one month 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 considered 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 to disclose information then Safeguarding priorities will take precedence over data protection and subject access requests.

Appendix 3

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 and UK General Data Protection Regulation (the EU GDPR was incorporated into UK legislation, with some amendment, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020 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, whichever is later.

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 us 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 able to provide you with copies of the information you request, we nevertheless reserve the right, to 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

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:

Please email a copy of this form to the DPO dpo@bdmat.org.uk

Appendix -4

Birmingham Diocesan Multi-Academy Trust

Personal Data Breach Procedures

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

1. On finding or causing a breach, or potential breach, the staff member, governor, or data processor must immediately notify the data protection officer (DPO) by emailing dpo@bdmat.org.uk
2. The DPO will investigate the report and determine whether a breach has occurred. To decide, the DPO will consider whether personal data has been accidentally or unlawfully:
 - a. Lost
 - b. Stolen
 - c. Destroyed
 - d. Altered
 - e. Disclosed or made available where it should not have been
 - f. Made available to unauthorised people.

Staff and governors will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

3. If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the CEO, headteacher and the chair of the Local Academy Board.
4. The DPO will make all reasonable efforts to contain and minimise the impact of the breach. Relevant staff members or data processors should help the DPO with this where necessary, and the DPO should take external advice when required (e.g. from IT providers).
5. The DPO will assess the potential consequences (based on how serious they are and how likely they are to happen) before and after the implementation of steps to mitigate the consequences.

6. The DPO will work out whether the breach must be reported to the ICO and the individuals affected using the ICO's self-assessment tool.
7. The DPO will document the decisions (either way), in case the decisions are challenged at a later date by the ICO, or an individual affected by the breach. Documented decisions are stored on the trust's central computer system.
8. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website, or through its breach report line (0303 123 1113), within 72 hours of the school's awareness of the breach. As required, the DPO will set out:
 - a. A description of the nature of the personal data breach including, where possible:
 - i. The categories and approximate number of individuals concerned
 - ii. The categories and approximate number of personal data records concerned
 - b. The name and contact details of the DPO
 - c. A description of the likely consequences of the personal data breach
 - d. A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned
9. If all the above details are not yet known, the DPO will report as much as they can within 72 hours of the school's awareness of the breach. The report will explain that there is a delay, the reasons why, and when the DPO expects to have further information. The DPO will submit the remaining information as soon as possible
10. Where the school is required to communicate with individuals whose personal data has been breached, the DPO will tell them in writing. This notification will set out:
 - a. A description, in clear and plain language, of the nature of the personal data breach
 - b. The name and contact details of the DPO
 - c. A description of the likely consequences of the personal data breach

- d. A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
11. The DPO will consider, in light of the investigation and any engagement with affected individuals, whether to notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies
 12. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:
 - a. Facts and cause
 - b. Effects
 - c. Action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals)
 13. Records of all breaches will be stored on the Information Governance record
 14. The DPO and headteacher / Head of Department (for Central Team) will meet to review what happened and how it can be stopped from happening again. This meeting will happen as soon as reasonably possible, and a formal record of the meeting will be made
 15. The DPO will complete termly compliance checks in school alongside the Headteacher to assess recorded data breaches and identify any trends or patterns requiring action by the school to reduce risks of future breaches

Actions to minimise the impact of data breaches

We set out below the steps we might take to try and mitigate the impact of different types of data breach if they were to occur, focusing especially on breaches involving particularly risky or sensitive information. We will review the effectiveness of these actions and amend them as necessary after any data breach.

Sensitive information being disclosed via email (including safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the DPO as soon as they become aware of the error via dpo@bdmat.org.uk
- If the sender is unavailable or cannot recall the email for any reason, the DPO will ask the Central ICT Team to attempt to recall it from external recipients and remove it from the school's email system (retaining a copy if required as evidence)
- In any cases where the recall is unsuccessful or cannot be confirmed as successful, the DPO will consider whether it's appropriate to contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The DPO will endeavor to obtain a written response from all the individuals who received the data, confirming that they have complied with this request
- The DPO with the support of the Central ICT Team will carry out an internet search to check that the information has not been made public; if it has, we will contact the publisher/website owner or administrator to request that the information is removed from their website and deleted
- If safeguarding information is compromised, the DPO will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.