BDMAT
Birmingham Diocesan
Multi-Academy Trust

General Data Protection Regulations Policy

Issued: June 2018
Reviewed: Summer 2026
Next review due: Summer 2029

BDMAT
Birmingham Diocesan Multi-Academy Trust

Contents

1	Aims	3
2	Legislation and guidance	3
3	Data protection principles	3
4	Definitions	4-6
5	Roles and responsibilities	6-8
6	Collecting personal data	8-11
7	Sharing personal data	11-12
8	Subject access requests and other rights of individuals	12-15
9	Parental requests to see the educational record	15
10	CCTV	16
11	Photographs and videos	16-17
12	Data protection by design and default	17-18
13	Artificial Intelligence	18
14	Data security and storage of records	18-20
15	Disposal of records	20
16	Personal data breaches	20
17	Training	20
18	Monitoring arrangements	21
19	Accountability and Evidence of Compliance	21
	Appendices:	22
1	Responding to a SAR	22
2	Personal data breach procedure	24

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 and The 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.

2.6 This policy also reflects the expectations of the ICO's Accountability Framework and Age Appropriate Design Code (Children's Code).

3.0 Data protection principles

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

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.

4.0 Definitions

Term	Definition
Personal data	Any information relating to an identified, or identifiable, living individual. This may include the individual's: • Name (including initials) • Identification number • Location data • Online identifier, such as a username It may also include factors specific to the individual's physical, physiological,
Term	**Definition**
	genetic, mental, economic, cultural, or social identity.

Special categories of personal data	Personal data, which is more sensitive and so needs more protection, including information about an individual's: • 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
Processing	Anything done to personal data, such as collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing, or destroying. Processing can be automated or manual.
Change Advisory Board	Members of the Executive Team with responsibility for Education and Operations who oversee any changes to the use of IT systems and hardware across the Trust.
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. BDMAT processes personal information relating to the pupils, staff, and visitors, and therefore, is a data controller.

	BDMAT is registered as a data controller with the Information Commissioner's Office and renews this registration annually legally required.
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
GDPR Champion	Individual nominated within school (or central team) with delegated responsibility for GDPR compliance and responsibility for all record keeping
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data

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 be subject to disciplinary action.

5.1 The Trust Board

The BDMAT Board of Directors has overall responsibility for ensuring that BDMAT and its schools comply with all relevant data protection obligations

5.2 Data Protection Officer (DPO)

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.

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.

The DPO will provide an annual report of their activities directly to the of Directors and, where relevant, report their advice and recommendations on school data protection issues. 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.

5.3 Leadership (**The Executive Team, Headteacher** and Heads of Department)

Day-to-day responsibilities for data in schools lies with the Headteacher, but may be discharged through GDPR Leads and GDPR Champions

Centrally the day-to-day responsibilities rest with the Executive Team, but may be discharged through Heads of Departments.

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:

- 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

- 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
- Setting up any contracts or sharing personal data with third parties

5.5 Staff Data Handling – Expected Practice

All staff must handle personal data in a secure and professional manner at all times.

Staff must:

- Only access personal data where necessary for their role
- Ensure emails containing sensitive information are **secure, accurate, and sent only to intended recipients**
- Double-check recipient details before sending emails
- Lock screens and devices when not in use
- Store paper records securely and not leave them unattended
- Report any suspected data breach immediately

Staff must not:

- Use personal devices or unapproved platforms to store or process personal data
- Share personal data via informal channels (e.g. personal email, messaging apps)
- Download or retain data longer than necessary
- Take photographs or videos of pupils on personal devices

Failure to follow these expectations may result in disciplinary action.

6.0 Collecting personal data

6.1 Lawfulness, fairness, and transparency

BDMAT only process personal data according to the 6 'lawful bases' (legal reasons) to do so as set out in data protection legislation.

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

    - 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

For special categories of personal data, BDMAT will ensure that one of the special category conditions for processing as set out in data protection law has been met:

- 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

- 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 personal data is first collected directly from individuals BDMAT will provide them with the relevant information required by data protection law.

BDMAT will always consider the fairness of data processing. BDMAT will ensure personal data is not handled in ways that individuals would not reasonably expect or use personal data in ways which have unjustified adverse effects on them.

6.2 Limitation, minimisation, and accuracy

BDMAT will only collect personal data for explicit and legitimate reasons and will explain these reasons to the individuals when their data is first collected.

BDMAT will inform individuals where the intention is to use their personal data for reasons other than those given in the original consent. BDMAT will inform the individuals concerned before processing their data and will obtain consent where required.

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

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

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

The schools within BDMAT will ensure that only the minimum necessary personal data is collected and used.

In practice:

- Staff must only collect and share information that is **directly relevant to their role**
- Emails and reports should avoid **unnecessary personal details**
- Personal data should not be copied to multiple recipients without clear justification
- Data should be anonymised where possible

Regular checks will be carried out to ensure adherence to these principles.

6.3. Protection of Children's Data (Children's Code)

BDMAT complies with the ICO's Age Appropriate Design Code and recognises that children require enhanced protection when their personal data is used.

The schools will ensure:

- Personal data relating to pupils is processed with **the best interests of the child as a primary consideration**
- Only the **minimum amount of data necessary** is collected and used
- Digital systems and platforms used by pupils are assessed for **privacy and safety risks**
- Privacy information is provided in a way that is **clear and age-appropriate**
- Data is not used for **profiling, tracking, or marketing purposes** without a lawful basis

Any online or digital services used by the school must:

- Be approved through the school's data protection processes
- Have appropriate **data processing agreements** in place
- Demonstrate compliance with UK GDPR and safeguarding expectations

7.0 Sharing personal data

7.1 BDMAT will not normally share personal data with anyone else without consent, except in certain circumstances where required to do so. These circumstances 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
- BDMAT need to liaise with other agencies. In such circumstances, where possible, consent will be obtained in advance

- Suppliers or contractors need data to enable services to be provided to staff and pupils. When doing this, BDMAT will:
    - Only appoint suppliers or contractors who 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
    - Only share data that the supplier or contractor needs to carry out their service

7.2 BDMAT will share personal data with law enforcement and government bodies where we are legally required to do so.

7.3 BDMAT uses third-party providers (including educational technology platforms) to support teaching and operational functions.

7.4 BDMAT may share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any pupils or staff.

7.5 Where personal data is transferred internationally BDMAT will do so in accordance with UK data protection law.

Before introducing any new system, the school will:

- Carry out appropriate **due diligence checks**
- Ensure a **Data Processing Agreement (DPA)** is in place
- Conduct a **Data Protection Impact Assessment (DPIA)** where required
- Assess safeguarding and data security risks

Only systems approved by the school or Trust may be used to process personal data.

Staff must not:

- Sign up to or use new platforms involving personal data without approval
- Upload personal data to external tools without authorisation

8.0 Subject access requests and other rights of individuals

8.1 **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

It is preferable that subject access requests are submitted in written form as this ensures there is a clear record of the request.

All subject access request received, in any form, must immediately be notified to the DPO.

- 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
- The safeguards provided if the data is being transferred internationally
- Subject access requests can be submitted in any form to the Trust and should include:
    - Name of individual
    - A correspondence address
    - A contact number and email address
    - Details about the information requested

8.2 **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 schools 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.

8.3 **Responding to subject access requests: (Please see Appendix 1 for further guidance)**

1) When responding to requests BDMAT:

- 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
- May ask the individual to provide 2 forms of identification ○ May contact the individual via phone to confirm the request was made ○ Will inform the individual regarding timescales, including where a request is complicated or numerous is likely to require an extension to be completed. BDMAT will inform the individual of the need and reason for an extension within 1 month of the receipt of the request.
- 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;
- 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.

2) BDMAT 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.

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

4) If BDMAT refuse a request the individual will be informed of the reason and informed about their right to complain to the ICO or to seek to enforce their subject access right through the courts.

8.4 **Other data protection rights of the individual**:

In addition to the right to make a subject access request (see above) and to receive information about how BDMAT 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 for their personal data to be to corrected, erased or processing of their personal data restricted (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
- 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.

9.0 Parental requests to see the education record

9.1 Parents of pupils at schools within BDMAT do not have an automatic legal right to access their child's educational record. BDMAT will, 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.

9.2 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.

10.0 CCTV

BDMAT uses CCTV in various locations around school sites to ensure it remains safe. BDMATs use of CCTV will adhere to the ICO's code of practice for the use of CCTV. Please refer to the CCTV policy for further information.

11.0 Photographs and videos

As part of school activities, BDMAT may take photographs and record images of individuals

11.1 **In our primary schools:**

BDMAT will obtain consent from parents/carers for photographs and videos to be taken of their child for communication, marketing, and promotional materials via Arbor. BDMAT 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, BDMAT 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:

BDMAT will obtain 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 parental consent is needed, BDMAT will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Where parental consent is not needed, BDMAT 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, BDMAT 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.

11.3 **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
- Online on our school website or social media pages

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

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

12.0 Data protection by design and default.

BDMAT 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)
- Having a Change Enablement Process in place which requires the completion of change requests to the BDMAT Change Advisory Board (CAB) so that full assessments of whether a full data protection impact assessments (DPIA) is required when introducing new technologies. Where the school's processing of personal data presents a high risk to rights and freedoms of individuals, a DPIA will be undertaken. The Head of IT and 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; BDMAT will also keep a record of attendance
- Regularly conducting reviews and audits to test BDMAT privacy measures to ensure compliance
- Appropriate safeguards being put in place for the transfer of any personal data outside of the UK, where different data protection laws may apply
- Maintaining records of all processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of our school and DPO and all information BDMAT are required to share about how personal data if used and processed (via our privacy notices)

For all personal data held, BDMAT will maintain an internal record of the type of data, type of data subject, how and why the data is being used, 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.

- The MAT and schools within it maintains clear and accessible **privacy notices for staff, pupils, and parents**, which are reviewed annually and reflect current data processing activities.

13.0 Artificial Intelligence (AI) and Automated Decision-Making

BDMAT recognises the increasing use of artificial intelligence (AI), automated systems, and data-driven technologies in education.

The schools will ensure that:

- Any use of AI systems (e.g. behaviour monitoring, safeguarding alerts, assessment tools, or administrative automation) is **lawful, fair, and transparent**
- A **Data Protection Impact Assessment (DPIA)** is conducted before introducing any AI or automated system that processes personal data
- Systems do not make **significant decisions about individuals without meaningful human involvement**
- Personal data used in such systems is **accurate, relevant, and limited to what is necessary**
- Any risks of bias, profiling, or unfair treatment are actively assessed and mitigated

Staff must:

- Not use unapproved AI tools that process personal data (e.g. uploading pupil information into external platforms)
- Seek approval from the Headteacher or DPO before using new digital or AI-based tools

14.0 Data security and storage of records (This section should be read in conjunction with the BDMAT IT Security Policy

BDMAT 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 securely when not in use.
- Papers containing confidential personal information will only be available where there is a clear medical reason and that there is explicit written consent., for example allergy advice in school kitchens.
- The Headteacher may authorise staff to take or keep school laptops off sit, if they are required to complete duties within their professional role. Personal data should not be stored on these devices.
- 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)

14.1 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, for example, we will shred or incinerate paper-based records and override or delete electronic files.

14.2 We may use third parties 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.

The school retains personal data only for as long as necessary to fulfil the purpose for which it was collected, in accordance with the UK GDPR principles of storage limitation and accountability.

Retention periods are determined by:

- Legal obligations
- Statutory guidance (including DfE guidance)
- Safeguarding requirements
- Operational need

Personal data will be securely deleted, destroyed, or anonymised when it is no longer required.

Indicative Retention Schedule

Data Type	Retention Period
Pupil educational records	Until pupil is age 25
Safeguarding/child protection	Until pupil is age 25 (or longer if required)

Attendance registers	3 years
Behaviour records	Date of incident + 3 years
Accident reports (students)	Until age 21
Accident reports (staff)	7 years
Staff personnel files	6 years after employment ends
Recruitment records (unsuccessful candidates)	6 months
SEN records	Until pupil is age 25
CCTV footage	Typically 30 days (unless required longer)
Emails containing personal data	Retained only as long as necessary
Complaints and investigations	6 years after resolution

- Staff must **not retain personal data longer than necessary**
- Data stored locally (e.g. desktops, emails) must be regularly reviewed and deleted
- Records must be disposed of securely (e.g. shredding, secure deletion)
- Digital systems must comply with retention rules set out by the Trust

Retention schedules are reviewed regularly by the CEO and Data Protection Officer.

15.0 Disposal of records

15.1 Personal information that is no longer needed will be disposed of securely.

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 2.

16.3 When appropriate, we will report the data breach to the ICO within 72 hours after becoming aware of it.

17.0 Training

17.1 All staff, governors and Directors will be provided with data protection training as part of their induction.

17.2 Data protection will also form part of continuing professional development.

17.3 All staff must complete **annual data protection refresher training**, and completion is monitored and recorded centrally.

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

19.0 Accountability and Evidence of Compliance

The schools within BDMAT will maintain clear evidence to demonstrate compliance with data protection law.

This includes:

A **Record of Processing Activities (RoPA)**

- A log of **data breaches and near misses**
- Records of **Data Protection Impact Assessments (DPIAs)**
- Staff training records and completion rates
- Regular internal audits of data protection practices

The Headteacher and DPO will review compliance on a **termly basis**, and findings will inform school improvement and risk management.

Appendix 1

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. Subject Access Requests can be made in any form, but it is preferable requests are written to ensure they are accurately recorded and can be responded to appropriately. For ease of request schools can provide an online form for the request to be submitted. This will ensure all information required for the request to be processed is provided. If the initial request does not clearly identify the information required, then further enquiries will be made to confirm this.
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
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, the response time is 30 calendar

days. However, the 30 calendar day period will not commence until the information requested has been confirmed and the identity of the requestor verified.

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 need to be obtained. The statutory timescale of 30 calendar days 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

The Data Protection Act 2018 and UK GDPR do not prevent the sharing of information for the purposes of keeping children safe. Fears about sharing information must not be allowed to stand in the way of the need to safeguard and promote the welfare and protect the safety of children.

Appendix 2

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 alongside the Headteacher/GDPR Champion and determine whether a breach has occurred. The decision will be based on 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.

   The headteacher, with the support of 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 Headteacher with this where necessary. Specialist and/or technical advice for example from the BDMAT IT Team will be available where required.

3. The Headteacher/GDPR Champion with the support of 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. If a breach has occurred or it is considered to be likely that is the case, the DPO will alert the CEO.
4. The DPO will support the Headteacher/ GDPR Champion in assessing whether the breach must be reported to the ICO and the individuals affected using the ICO's self- assessment tool.

5. The DPO will ensure the school documents 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 centrally by BDMAT's.
6. Where the ICO must be notified, the Headteacher/GDPR Champion 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
7. If all the above details are not yet known, the Headteacher/GDPR Champion 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 school expects to have further information. The Headteacher/GDPR Champion will submit the remaining information as soon as possible
    a. The name and contact details of the DPO
    b. A description of the likely consequences of the personal data breach
    c. 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.
8. Where the school is required to communicate with individuals whose personal data has been breached, the Headteacher/GDPR Champion 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

9. Following the investigation and other engagement with affected individuals the Headteacher, with the support of the DPO, will consider, 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
10. The Headteacher/GDPR Champion will document each breach, irrespective of whether it is reported to the ICO on the Information Governance record.

    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)

12. 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

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

- Sensitive information being disclosed via email 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 BDMAT IT 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 Headteacher with the support of 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 endeavour 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 BDMAT IT Team, will carry out an internet search to check that the information has not been made public; if it has BDMAT 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 Headteacher will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its 3 local safeguarding partners.