Data Protection & GDPR Policy 2021

The Midland Academies Trust

Data Protection Officer

Contents

Data Protection & GDPR Policy 2021

Data Protection & GDPR Policy 2021

1. Introduction

1.1 The Midland Academies Trust (the "Trust") is a multi-academy trust with exempt charity status. The Trust's academies are:

i. Hartshill School;

ii. The George Eliot School;

iii. The Nuneaton Academy; and

iv. Heath Lane Academy.

1.2 This Policy defines the Trust's responsibilities in respect of data protection and the collection and use of information and personal data.

1.3 The Trust aims to ensure that all the personal data it holds about staff, students, parents, visitors, Directors, Raising Achievement Board members and other individuals, is collected, stored and processed in accordance with the General Data Protection Regulation (GDPR). This Policy applies to all personal data, regardless of whether it is in paper or electronic format.

1.4 In this Policy, all references to "we" and "our" refer to the Trust, unless distinguished in the text.

2. Definitions

2.1 'Personal Data' is defined as information about a living individual, held either electronically or manually as an accessible record or records, from which the person can be identified.

2.2 Examples of personal data which may be used by the Trust in its day to day activities include, names, addresses (email and property addresses), telephone numbers and other contact details, educational records, CVs, performance reviews, payroll information and images obtained through CCTV.

2.3 'Data Processing' is defined as the obtaining, recording, holding, organising, adapting, altering, retrieving, consulting, matching, transmitting, disseminating, making available, aligning, combining, blocking, erasing or destroying of data as defined above.

2.4 'Data Subject' is defined as a living person about whom data is processed.

2.5 'Automated Data' is personal data held on computer and automatically processed, such as automatic scoring, document image processing, CCTV or identity photos.

2.6 'Manual Records' are records containing personal data organised in such a way as a living individual may be identified, whether from those records alone or in combination with others.

2.7 'Sensitive Personal Data' is referred to in the GDPR as 'special categories of personal data' such as genetic data, biometric data, political views, race and ethnicity and where collected, should not be used unless strictly necessary.

2.8 Terms and Definitions:

Term	Definition
Personal Data	Any information relating to an identified, or identifiable, individual. This may include the individual's: - name (including initials); - identification number; - location data; - online identifier, such as a username.

Term	Definition
	It may also include factors specific to the individual's physical, physiological, 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.
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 personal 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.
Individual Rights	Data subjects (who include staff) have a range of individual rights as set out in the GDPR and the Trust's Rights of Individuals under the GDPR Policy

3. Related Policies and Documents

3.1 Rights of Individuals under the GDPR Policy;

3.2 Rights of Individuals under the GDPR Procedure.

3.3 Freedom of Information Policy.

3.4 Safeguarding Policy.

3.5 Public Interest Disclosure (Whistleblowing) Policy.

3.6 IT Security Policy.

3.7 BYOD Policy

3.8 Other policies and documents may be identified from time-to-time as circumstances change and may be added to this list.

4. Rationale

4.1 The Trust is required to comply with the obligations and requirements set out in the GDPR and the Data Protection Act (DPA).

4.2 This Policy is intended to ensure that personal information is dealt with appropriately and in accordance with the legislation.

4.3 The Trust requires all staff to comply with this Policy. Non-compliance puts data subjects, whose personal data is being processed, at risk. It also carries the risk of the imposition of significant civil and criminal sanctions for the individual and the Trust. Consequently, any failure to comply with this Policy may lead to disciplinary action which could result in dismissal for gross misconduct. If a non-employee breaches this Policy, they may have their contract terminated with immediate effect.

5. Legislation and Guidance

5.1 This Policy meets the requirements of the:

i. GDPR and is based on guidance published by the ICO and the ICO's code of practice for subject access requests; and

ii. Protection of Freedoms Act 2012 when referring to our use of biometric data.

5.2 The Policy also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

6. Core Principles

6.1 The principles set out in the GDPR must be adhered to when processing personal data. The principles are as follows:

i. Personal Data shall be processed fairly and lawfully.

ii. Personal Data shall be obtained only for specified and lawful purposes and shall not be processed in a way that is incompatible with those purposes or in contradiction to the GDPR.

iii. Personal Data shall be adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

iv. Personal Data shall be accurate and kept up to date.

v. Personal Data shall be processed in accordance with the data subjects' rights.

vi. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against the accidental loss or destruction of, or damage to personal data.

vii. Personal Data shall not be transferred outside of the EU except in circumstances defined in the Act and with approval from the Trust's Data Protection Officer (DPO) or the IT Services Manager.

7. The Data Controller

7.1 The Trust processes personal data relating to students, parents, staff, visitors and others, and therefore is a data controller.

7.2 The Trust is registered with the ICO as a data controller and will renew this registration annually or as otherwise legally required.

8. Roles and Responsibilities

8.1 **Policy Applicability**: this Policy applies to all staff employed by the Trust, and to external organisations or individuals working on its behalf. Staff who do not comply with this Policy may face disciplinary action.

8.2 **The Board of Directors:** has overall responsibility for ensuring that the Trust complies with all relevant data protection obligations.

8.3 **Data Protection Officer (DPO):**

8.3.1 Is responsible for overseeing the implementation of this Policy, monitoring Trust compliance with data protection law, and developing related policies and guidelines where applicable.

8.3.2 Will provide an annual report of their activities to the Board and, where relevant, report to the Board on their advice and recommendations about data protection issues.

8.3.3 Is the first point of contact for individuals whose data the Trust processes, and for the ICO.

8.3.4 Is contactable via telephone: 02476 243000 or email: dpo@midlandacademiestrust.co.uk

8.4 **Principal and Chief Executive**: acts as the representative of the data controller on a day-to-day basis.

8.5 **All Staff** are responsible for:

8.5.1 Collecting, storing and processing any personal data in accordance with this Policy.

8.5.2 Informing the academy they work at of any changes to their personal data, such as a change of address.

8.5.3 Contacting the DPO in the following circumstances:

i. With any questions about the operation of this Policy, data protection law, retaining personal data or keeping personal data secure.

ii. If they have any concerns that this Policy is not being followed.

iii. If they are unsure whether or not they have a lawful basis to use personal data in a particular way.

iv. If they need to rely on or capture consent, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area.

v. If there has been a data breach.

vi. Whenever they are engaging in a new activity that may affect the privacy rights of individuals.

vii. If they need help with any contracts or sharing personal data with third parties.

9. Information Security

9.1 The Trust will use appropriate technical and organisational measures to keep personal information secure, to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9.2 All staff are responsible for keeping information secure in accordance with the legislation and must follow the Trust's Acceptable Usage Policy.

9.3 The Trust will develop, implement and maintain safeguards appropriate to its size, scope and business, its available resources, the amount of personal data that it owns or maintains on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). The Trust will regularly evaluate and test the effectiveness of those safeguards to ensure security of processing.

9.4 Staff must guard against unlawful or unauthorised processing of personal data and against the accidental loss of, or damage to, personal data. Staff must exercise particular care in protecting sensitive personal data from loss and unauthorised access, use or disclosure.

9.5 Staff must follow all procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. Staff may only transfer personal data to third-party service providers who agree in writing to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

9.6 Staff must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

i. Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it.

ii. Integrity means that personal data is accurate and suitable for the purpose for which it is processed.

iii. Availability means that authorised users can access the personal data when they need it for authorised purposes.

9.7 Staff must comply with and not attempt to circumvent the administrative, physical and technical safeguards the Trust has implemented and maintains in accordance with the GDPR and DPA.

9.8 Where the Trust uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. Contracts with external organisations must provide that:

i. the organisation may only act on the Trust's written instructions;

ii. those processing data are subject to the duty of confidence;

iii. appropriate measures are taken to ensure the security of processing;

iv. the organisation will assist the Trust in providing subject access and allowing individuals to exercise their rights in relation to data protection;

v. the organisation will delete or return all personal information to the Trust as requested at the end of the contract;

vi. the organisation will submit to audits and inspections, provide the Trust with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Trust immediately if it does something infringing data protection law.

9.9 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant staff must seek advice from the DPO and complete third part due diligence and a DATA PROTECTION IMPACT ASSESSMENT.

10. Collecting Personal Data - Lawfulness, Fairness and Transparency

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

i. The data needs to be processed so that the Trust can fulfil a **contract** with the individual, or the individual has asked the Trust to take specific steps before entering into a contract.

ii. The data needs to be processed so that the College can comply with a **legal obligation.**

iii. The data needs to be processed to ensure the **vital interests** of the individual e.g. to protect someone's life.

iv. The data needs to be processed so that the College, as a public authority, can perform a task in the **public interest**, and carry out its official functions.

v. The data needs to be processed for the **legitimate interests** of the College or a third party (provided the individual's rights and freedoms are not overridden).

vi. The individual (or their parent/carer when appropriate in the case of a student under 13) has freely given clear **consent.**

10.2 In respect of special categories of personal data, we will also meet one of the special category conditions for processing that data. These conditions are set out in the GDPR.

10.3 If we offer online services to students, such as classroom apps, and we intend to rely on consent as a basis for processing personal data, we will obtain parental consent where the student is under 13.

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

11. Limitation, Minimisation and Accuracy

11.1 We will only collect personal data for specified, explicit and legitimate reasons. It must not be further processed in any manner incompatible with those proposed. We will explain these reasons to the individuals when we first collect their data.

11.2 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.

11.3 Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processes. Staff may only process data when their role required it. Staff must not process personal data for any reason unrelated to their role.

11.4 When staff no longer need the personal data they hold, they must ensure it is deleted or anonymised.

12. Sharing Personal Data

12.1 We will not normally share personal data with anyone else, but may do so where:

i. there is an issue with a student or parent/carer that puts the safety of our staff at risk;

ii. we need to liaise with other agencies.

12.2 Our suppliers or contractors need data to enable us to provide services to our staff and students; for example, IT companies. To provide safeguards, we will:

i. only appoint suppliers or contractors that can provide sufficient guarantees that they comply with data protection law;

ii. establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data we share.

iii. only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us.

12.3 We will also share personal data with law enforcement and government bodies where we are legally required to do so, including for example:

i. the prevention or detection of crime and/or fraud;

ii. the apprehension or prosecution of offenders;

iii. the assessment or collection of tax owed to HMRC;

iv. in connection with legal proceedings;

v. where the disclosure is required to satisfy our safeguarding obligations;

vi. research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided.

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

12.5 Where we transfer personal data to a country or territory outside the European Economic Area, we will do so in accordance with data protection law. The DPO will be made aware of any need to transfer data before the transfer takes place, to ensure that it complies with the GDPR.

13. Subject Access Requests

13.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust e holds about them. This includes:

i. confirmation that their personal data is being processed;

ii. access to a copy of the data;

iii. the purposes of the data processing;

iv. the categories of personal data concerned;

v. who the data has been, or will be, shared with;

vi. how long the data will be stored for, or if this is not possible, the criteria used to determine this period;

vii. the source of the data, if not the individual;

viii. whether any automated decision-making is being applied to their data, and what the significance and consequences of this might be for the individual.

13.2 Subject access requests must be submitted in writing, by either letter, email or fax to the DPO. They should include:

i. name of individual;

ii. correspondence address;

iii. contact number and email address;

iv. details of the information requested.

13.3 If staff receive a subject access request they must immediately forward it to the DPO.

13.4 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.

13.5 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 students in our College may not be granted without the express permission of the student. This is not a rule and a student's ability to understand their rights will always be judged on a case-by-case basis.

13.6 When responding to requests, we:

i. may ask the individual to provide 2 forms of identification;

ii. may contact the individual via phone to confirm the request was made;

iii. will respond without delay and within 1 month of receipt of the request;

iv. will provide the information free of charge;

v. may tell the individual we will comply within 3 months 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.

13.7 We will not disclose information if it:

i. might cause serious harm to the physical or mental health of the pupil or another individual;

ii. would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests;

iii. is contained in adoption or parental order records;

iv. is given to a court in proceedings concerning the child;

v. if the request is unfounded or excessive, we may refuse to act on it, or charge a reasonable fee that takes into account administrative costs.

13.8 A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

13.9 When we refuse a request, we will inform the individual to the reason for the refusal and that they have the right to complain to the ICO.

14. Other Data Protection Rights of the Individual

14.1 in addition to the right to make a subject access request, and to receive information when we are collecting their data about how we use and process it, individuals have the right to:

i. Withdraw their consent to processing at any time.

ii. Ask us to rectify, erase or restrict processing of their personal data, or object to the processing of it (in certain circumstances).

iii. Prevent use of their personal data for direct marketing.

iv. Challenge processing which has been justified on the basis of public interest.

v. Request a copy of agreements under which their personal data is transferred outside of the European Economic Area.

vi. Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement that might negatively affect them).

vii. Prevent processing that is likely to cause damage or distress.

viii. Be notified of a data breach in certain circumstances.

ix. Make a complaint to the ICO.

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

14.2 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.

15. Biometric Recognition Systems

15.1 Where we use biometric data as part of an automated biometric recognition system we will comply with the requirements of the Protection of Freedoms Act 2012.

15.2 Parents/carers will be notified before any biometric recognition system is put in place, or before their child first takes part in it if the child is under 13. The Trust will obtain written consent from at least one parent or carer before we take any biometric data from their child and first process it.

15.3 Parents/carers, children and students have the right to choose not to use the Trust's biometric system(s), once in place. We will provide alternative means of accessing the relevant services for those individuals.

15.4 Parents/carers and students can object to participation in the Trust's biometric recognition system(s), once in place, or withdraw consent, at any time, and we will make sure that any relevant data already captured is deleted.

15.5 As required by law, if a student refuses to participate in, or continue to participate in, the processing of their biometric data, we will not process that data irrespective of any consent given by the child's parent(s)/carer(s).

15.6 Where staff members or other adults use the biometric system(s), we will also obtain their consent before they first take part in using the system and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the Trust will delete any relevant data already captured.

16. CCTV

16.1 We use CCTV in various locations around the Trust premises to ensure safety and security. The trust adheres to the ICO's code of practice for the use of CCTV.

16.2 There is no requirement to ask individuals' permission to use CCTV, but we make it clear when and where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use.

16.3 Any enquiries about the CCTV system should be directed to the School Business Managers.

17. Photographs and Images

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

17.2 Unless prior consent has been obtained from parents/students/staff, the Trust will not utilise such images for publication or communication to external sources.

18. Data Protection by Design

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

i. Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge.

ii. 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 8).

iii. Completing privacy impact assessments where the Trust's processing of personal data presents a high risk to the rights and freedoms of individuals and when new technologies.

iv. Integrating data protection into internal documents including this Policy, any related Policies, documents and privacy notices.

v. Regularly training members of staff on data protection law, this Policy, any related Policies, documents and any other data protection matters; we will also keep a record of the training which has been delivered.

vi. Regularly conducting reviews and audits to test our privacy measures and make sure we are compliant.

18.2 Maintaining records of our processing activities, including:

i. For the benefit of data subjects, making available the name and contact details of our Trust and DPO and all information we are required to share about how we use and process their personal data (via our privacy notices).

ii. For all personal data that we hold, maintaining an internal record of the type of data, data subject, how and why we are using the data, any third-party recipients, how and why we are storing the data, retention periods and how we are keeping the data secure.

19. Data Security and Storage of Records

19.1 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.

19.2 Personal data should not be retained for any longer than is necessary. The length of time data should be retained will depend on a number of circumstances including the reasons why personal data was obtained.

19.3 Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept securely when not in use.

19.4 Papers containing confidential personal data must not be left on office and classroom desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access.

19.5 Passwords are used to access College computers, laptops and other electronic devices. Staff and students are reminded to change their passwords at regular intervals.

19.6 Access to USB storage is not allowed unless appropriate encryption software deemed is used to protect the device and its content.

19.7 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.

20. Disposal of Records

20.1 Personal data 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.

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

21. Data Breaches

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

21.2 In the unlikely event of a suspected data breach, we will follow the procedure set out in Appendix 1.

21.3 When appropriate, we will report the data breach to the ICO within 72 hours.

21.4 Staff must ensure they inform their line manager and the DPO immediately on discovering a data breach and make all reasonable efforts to recover the data.

22. Training

22.1 All staff are provided with data protection training as part of their induction process.

22.2 Data protection will form part of continuing professional development, where changes to legislation, guidance or the Trust's processes make it necessary.

23. Monitoring and Review

23.1 The DPO is responsible for monitoring and reviewing this Policy.

23.2 This Policy will be reviewed every three years and updated, as applicable, to ensure that it remains fit for purpose in the light of any relevant changes to the law, organisational policies, contractual obligations or as directed by the Chief Executive.

Appendix 1

Data Breach Procedure

1. This procedure is based on guidance on personal data breaches produced by the ICO.
2. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify their line manager and the DPO.
3. The DPO will investigate the report and determine whether a breach has occurred. To make such a decision, the DPO will consider whether personal data has been accidentally or unlawfully:
    i. lost;
    ii. stolen;
    iii. destroyed;
    iv. altered;
    v. disclosed or made available where it should not have been;
    vi. made available to unauthorised people.
4. The DPO will alert the Executive Principal / Chief Executive Officer.
5. The DPO will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors, where necessary.
6. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen.
7. The DPO will decide whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. In making this decision, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), due to:
    i. the loss of control over their data;
    ii. discrimination;
    iii. identify theft or fraud;
    iv. financial loss;
    v. unauthorised reversal of pseudonymisation (for example, key-coding);
    vi. damage to reputation;
    vii. doss of confidentiality;
    viii. any other significant economic or social disadvantage to the individual(s) concerned.
8. If it is likely that there will be a high risk to people's rights and freedoms, the DPO must notify the ICO.
9. The DPO will document the decision in case it is later challenged by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's Data Breach Register.
10. The DPO will notify the ICO within 72 hours. As required, the DPO will set out:
    i. A description of the nature of the personal data breach including, where possible the categories and approximate number of individuals concerned, and the categories and approximate number of personal data records concerned.
    ii. The name and contact details of the DPO.
    iii. A description of the likely consequences of the personal data breach.
    iv. 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.
11. If any of the above details are not known, the DPO will report as much as they can within 72 hours. 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.

12. The DPO will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the DPO will identify a member / members of staff to promptly inform all individuals whose personal data has been breached. This notification will set out:

    i. The name and contact details of the DPO.

    ii. A description of the likely consequences of the personal data breach.

    iii. 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.

13. The DPO will identify a member / members of staff to notify any relevant third parties who can help mitigate the loss to individuals; for example, the police, insurers, banks or credit card companies.

14. The DPO will document each breach, irrespective of whether it is reported to the ICO. For each breach, this record will include the:

    i. The facts concerning, and the cause of the breach.

    ii. The effects / impact of the breach.

    iii. The action taken to contain the breach and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals).