GDPR Data Protection Policy 2018

The Midland Academies Trust

MAT Business & Quality Assurance Manager

Contents

GDPR Data Protection Policy 2018

Appendices

GDPR Data Protection Policy 2018

1. Introduction

1.1 The Midland Academies Trust and its schools (the "**Trust**") is an independent charitable organisation established by North Warwickshire & Hinckley College, a Department for Education approved academy sponsor, to support local schools. The Trust's schools include:

i. Hartshill School

ii. The George Eliot School

iii. The Nuneaton Academy

iv. Heath Lane Academy

1.2 The Trust aims to ensure that all personal data collected about staff, pupils, parents, Raising Achievement Board (RAB) Members, visitors 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.

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

2. Applicable Data

2.1 For the purpose of this policy, personal data refers to information that relates to an identifiable, living individual, including information such as an IP address. The GDPR applies to both automated personal data and to manual filing systems.

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 Sensitive Personal Data is referred to in 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.

3. Related Policies and Documents

3.1 Freedom of Information Policy

3.2 Safeguarding Policy

3.3 Public Interest Disclosure (Whistleblowing) Policy

4. Legislation and Guidance

4.1 This Policy meets the requirements of the GDPR and is based on guidance published by the Information Commissioner's Office (ICO) on the GDPR and the ICO's code of practice for subject access requests. It meets the requirements of the Protection of Freedoms Act 2012 when referring to our use of biometric data. It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

5. 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 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.

6. The Data Controller

6.1 Our Trust processes personal data relating to parents, pupils, staff, visitors and others, and therefore is a data controller.

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

7. Roles and Responsibilities

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

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

7.3 **Data Protection Officer (DPO)**

7.3.1 The 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.

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

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

7.3.4 The Trust's DPO is Val Hone and is contactable via telephone: 02476 243531 or email: val.hone@midlandacademiestrust.co.uk

7.3 **Principal:** acts as the representative of the data controller on a day-to-day basis.

7.4 **All Staff:**

7.4.1 Staff are responsible for collecting, storing and processing any personal data in accordance with this policy

7.4.2 Informing the school of any changes to their personal data, such as a change of address

7.4.3 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

8. Data Protection Principles

8.1 The GDPR is based on data protection principles that our Trust must comply with. The principles say that personal data must be:

i. Processed lawfully, fairly and in a transparent manner.

ii. Collected for specified, explicit and legitimate purposes.

iii. Adequate, relevant and limited to what is necessary to fulfil the purposes for which it is processed.

iv. Accurate and, where necessary, kept up to date.

v. Kept for no longer than is necessary for the purposes for which it is processed.

vi. Processed in a way that ensures it is appropriately secure.

8.2 This Policy sets out how the Trust aims to comply with these principles.

9. Collecting Personal Data

9.1 **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:

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 Trust 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 Trust, 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 Trust 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 pupil) has freely given clear **consent**

vii. For special categories of personal data, we will also meet one of the special category conditions for processing which are set out in the GDPR.

viii. If we offer online services to pupils, such as classroom apps, and we intend to rely on consent as a basis for processing, we will get parental consent where the pupil is under 13

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

9.2 **Limitation, minimisation and accuracy**

i. 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.

ii. 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.

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

iv. 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 Information and Records Management Society's toolkit for schools

10. Sharing Personal Data

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

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

ii. We need to liaise with other agencies

10.2 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:

i. Only appoint suppliers or contractors which 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

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

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

10.4 Research and statistical purposes, as long as personal data is sufficiently anonymised or consent has been provided

10.5 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.

10.6 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.

11. Subject Access Requests

11.1 Individuals have a right to make a 'subject access request' to gain access to personal information that the Trust 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 isn't 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

11.2 Subject access requests must be submitted in writing, either by 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

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

11.4 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.

11.5 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 pupils in our Trust 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.

11.6 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.

11.7 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 which takes into account administrative costs.

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

11.8 When we refuse a request, we will tell the individual why, and tell them they have the right to complain to the ICO.

12. Other Data Protection Rights of The Individual

12.1 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 9), individuals also 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)

xi. 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.

13. Biometric Recognition Systems

13.1 Where we use pupils' biometric data as part of an automated biometric recognition system (for example, pupils use finger prints to receive school dinners instead of paying with cash), we will comply with the requirements of the Protection of Freedoms Act 2012.

13.2 Parents/carers will be notified before any biometric recognition system is put in place or before their child first takes part in it. The school will get written consent from at least one parent or carer before we take any biometric data from their child and first process it.

13.3 Parents/carers and pupils have the right to choose not to use the school's biometric system(s). We will provide alternative means of accessing the relevant services for those pupils.

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

13.5 As required by law, if a pupil 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 pupil's parent(s)/carer(s).

13.6 Where staff members or other adults use the school's biometric system(s), we will also obtain their consent before they first take part in it, 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 school will delete any relevant data already captured.

14. CCTV

14.1 We use CCTV in various locations around the school sites to ensure it remains safe. We will adhere to the ICO's code of practice for the use of CCTV.

14.2 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.

14.3 Any enquiries about the CCTV system should be directed to the School Business Manager.

15. Photographs and images

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

15.2 Unless prior consent from parents/pupils/staff has been given, the school shall not utilise such images for publication or communication to external sources.

16. Data Protection By Design

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

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

16.1.2 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).

16.1.3 Completing privacy 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.

16.1.4 Integrating data protection into internal documents including this policy, any related policies and privacy notices.

16.1.5 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 training.

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

12.1.7 Maintaining records of our processing activities, including:

i. 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).

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.

17. Data Security and Storage Of Records

17.1 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.

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

17.3 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

17.4 Passwords are used to access school computers, laptops and other electronic devices. Staff and pupils are reminded to change their passwords at regular intervals

17.5 Encryption software is used to protect all portable devices and removable media, such as laptops and USB devices

17.6 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 9)

18. Disposal of Records

18.1 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.

18.2 For example, 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 Trust's behalf. If we do so, we will require the third party to provide sufficient guarantees that it complies with data protection law.

19. Personal Data Breaches

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

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

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

20. Training

20.1 All staff, Directors and RAB members are provided with data protection training as part of their induction process.

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

21. Monitoring and Review Arrangements

21.1 The DPO is responsible for monitoring and reviewing this policy.

21.2 The Policy and associated documentation will be reviewed on a three yearly basis or as required by changes in the law, regulation or as directed by the Chief Executive.

Appendix 1

Personal Data Breach Procedure

This procedure is based on guidance on personal data breaches produced by the ICO.

1. On finding or causing a breach, or potential breach, the staff member or data processor must immediately notify the DPO
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:
    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.
3. The DPO will alert the Executive Principal and Chief Executive.
4. 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.
5. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen
6. The DPO will work out whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, 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), including through:
    i. 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. loss of confidentiality;
    viii. any other significant economic or social disadvantage to the individual(s) concerned.
7. If it's likely that there will be a risk to people's rights and freedoms, the DPO must notify the ICO.
8. The DPO will document the decision (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach. Documented decisions are stored on the Trust's Data Breach Register
9. Where the ICO must be notified, the DPO will do this via the 'report a breach' page of the ICO website 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;
        - 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.

10. If all the above details are not yet 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

11. 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 promptly inform, in writing, 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.

12. The DPO will notify any relevant third parties who can help mitigate the loss to individuals; for example, the police, insurers, banks or credit card companies

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

    i. facts and cause;

    ii. effects;

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