WELLSWAY
MULTI ACADEMY TRUST

Data Protection Policy

Table of Contents

1. Introduction

Wellsway Multi Academy Trust (WMAT) is fully committed to compliance with the requirements of the EU General Data Protection Regulation. The Trust will therefore aim to ensure that all employees, governors, Trustees, contractors, agents, consultants, or partners of the Trust who have access to any personal data held by or on behalf of the Trust, are fully aware of and abide by their duties and responsibilities under the Regulation.

2. Policy aims and objectives

The Trust needs to collect and use certain types of information about people with whom it deals in order to perform its functions. This includes information on current, past and prospective pupils and employees, suppliers, clients, customers, service users and others with whom it communicates. The Trust is required by law to collect and use certain types of information to fulfil its statutory duties and also to comply with the legal requirements of the Government. This personal information must be dealt with properly whether it is collected, recorded and used on paper, computer, or other material. There are safeguards to ensure this in the EU General Data Protection Regulation.

The Trust regards the lawful and correct treatment of personal information as critical to successful operations and to maintaining confidence between those with whom we deal and ourselves. It is essential that it treats personal information lawfully and correctly.

The purpose of this policy is to explain how the Trust will ensure compliance with the EU General Data Protection Regulation. It includes organisational measures and individual responsibilities which aim to ensure that the Trust complies with the data protection principles and respects the rights of individuals. This policy provides outline measures and puts in place a structure for monitoring compliance.

Detailed procedures and guidance do not form part of this overarching policy document. The detailed guidance are available in the supporting documents and related policies are listed in Section 15.

3. Legal Context and Definitions

3.1 Definitions

The EU General Data Protection Regulation (GDPR) governs how information about people (Personal Data) should be treated. It also gives rights to individuals whose data is held. The Regulation came into force on 25 May 2018 and applies to all personal data collected at any time whether held on computer or manual record. The Regulation is enforced by the Information Commissioner.

The GDPR makes a distinction between personal data and "sensitive" personal data. Sensitive personal data is subject to stricter conditions of processing.

- **Personal data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Sensitive personal data** is defined as personal data consisting of information as to: Racial or ethnic origin; political opinions; religious or philosophical beliefs; or trade union membership; genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual orientation.

A **Data Subject** is an individual who is the subject of the data.
A **Data Controller** is an organisation, or person that determines the purposes for which and the manner in which any personal data is to be processed.
A **Data processor** is any organisation or person who processes data on behalf of the data controller.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

3.2 The Principles of GDPR

The GDPR contains six principles for processing personal data with which organisations must comply:

- *Lawfulness , fairness and transparency* – personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject
- *Purpose limitation* - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- *Data minimisation* - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- *Accuracy* - accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- *Storage limitation* - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed
- *Integrity and confidentiality* - processed in a manner that ensures appropriate security of the personal data

All data subjects have the following rights:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information.
- The right to prevent processing in certain circumstances.
- The right to rectify, block or erase information which is regarded as wrong information.
- The right to have decisions reviewed where they have been made automatically.
- The right to object to receiving marketing information.

4. Scope

4.1 Context of this policy

This policy applies to all the Staff, Contractors and organisations / third parties that use personal data in support of their work on behalf of the Trust.

4.2 Personal data held

This policy applies to all processing of personal data held by the Trust. This includes:

- Personal data processed by the Trust.
- Personal data controlled by the Trust but processed by another organisation, on the Trust's behalf (for example private sector contractors; and Service Level Agreements with voluntary sector organisations).
- Personal data processed jointly by the Trust and its partners

The policy does not cover personal data held by the Local Authority or the Department for Education which are data controllers in their own right.

Personal data held by the Trust may be held in many forms including:

- Database records
- Computer files
- Emails
- Paper files
- CCTV and video recordings
- Sound recordings
- Photographs
- Microfiche and film
- Website
- Mobile phones

Data subjects may include:

- Current, past and prospective employees and pupils

- Parents and other pupil or staff contacts
- Suppliers
- Clients
- Others with whom the Trust communicates

5. Responsibilities

5.1 Organisational Responsibilities

WMAT is a data controller under the EU General Data Protection Regulation.

5.2 Individual Responsibilities

5.2.1 Every employee must comply with this policy. Failure to comply with the policy may result in disciplinary action which could include dismissal.

5.2.2 All contractors/ service providers must comply with the policy when using personal data supplied to / held by the Trust to facilitate the Commissioned Service being provided.

5.2.3 It is a criminal offence to access personal data held by the Trust for other than school business, or to procure the disclosure of personal data to a third party.

5.2.4 It is a further offence to sell such data.

5.2.5 Employees who access or use personal data held by the Trust for their own purposes will be in breach of relevant policies of the Trust, including but not limited to the Safer Working Practices Policy, e-Safety Policy, IT Security Policy and subject to disciplinary action, which could include dismissal, and may also face criminal proceedings.

6. Purposes of Processing Personal Data and Fairness

6.1 The Trust will collect and process personal data only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.

6.2 The Trust will use a condition of processing as detailed in Article 6(1) of the GDPR of their personal data:

6.2.1 the data subject has given consent to the processing of his or her personal data for one or more specific purposes

6.2.2 processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

6.2.3 processing is necessary for compliance with a legal obligation to which the controller is subject

6.2.4 processing is necessary in order to protect the vital interests of the data subject or of another natural person

6.2.5 processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

6.3 When sensitive data is collected, the Trust will use a condition of processing as detailed in Article 9 of the GDPR. These include protecting the vital interests of the data subject or meeting a legal obligation.

6.4 In cases where consent is obtained, the consent must be free and informed and may be changed at any time.

6.5 The Trust will, as far as is practicable, ensure that all individuals whose details are processed are aware of the way in which that information will be held, used and disclosed. Individuals will, where possible, be informed of the likely recipients of the information - whether the recipients are internal or external to the Trust.

6.6 This information will be provided when personal data is first collected, whether written or verbal.

6.7 When personal data is to be used for a new purpose then this information will be provided to the data subject again and if necessary a new consent will be sought.

6.8 People can ask for more details about how their personal data is being used at any time and if unhappy about how their data is used may make a complaint.

Any person whose details (including photographs) are to be included on the Trust or Trust school websites or other promotional materials will be asked to give written consent.

7. Data Quality, Integrity and Retention

7.1 The Trust's use of personal data will comply with GDPR.

7.2 Personal data held will be relevant to the stated purpose and adequate but not excessive.

7.3 The Trust will ensure, as far as is practicable, that the information held is accurate and up-to-date.

7.4 A data register will be held and maintained for all information assets containing personal data.

7.5 Each information asset will have a nominated owner. Though responsibility for the security measures may be delegated to a nominated individual, accountability remains with the owner.

7.6 An annual review of information assets held by each school or business service should be performed.

7.7 If personal data is found to be inaccurate, this will be remedied as soon as possible.

7.8 Personal information, such as contact details, may be shared within the Trust where it is necessary to keep records accurate and up-to-date, and in order to provide individuals with a better service.

7.9 Records may include professional opinions about individuals but employees will not record any personal opinions about individuals.

7.10 Information will only be held for as long as is necessary after which the details will normally be deleted. Where details of individuals are stored for long-term archive or historical reasons, and where it is necessary to retain the personal detail within the records, it will be done within the requirements of the legislation.

7.11 Redundant personal data will be destroyed using the Trust's procedure for disposal of confidential waste and in accordance with retention schedules.

8. Security

8.1 Any inappropriate, unauthorised access of data, use or misuse of data or failure to comply with IT security arrangements and policies may result in disciplinary action, including dismissal.

8.2 The Trust will implement appropriate technical and organisational security measures so that unauthorised staff and other individuals are prevented from gaining access to personal information.

8.3 An employee must only access personal data they need to use as part of their job. Inappropriate or unauthorised access may result in disciplinary action, including dismissal and criminal prosecution.

8.4 The Trust has an IT Security Policy which applies to electronic systems containing personal data.

8.5 All data breaches (however minor) must be reported via the process detailed in the Information Security Incident procedures.

8.6 All staff within the Trust will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

8.7 Manual files and other records or documents containing personal/sensitive data will be kept in a secure environment and accessed on a need-to-know basis only.

8.8 Personal data held on computers and computer systems will be installed with user-profile type password controls, encryption and where necessary, audit and access trails to establish that each user is fully authorised. Personal data should not be held on unencrypted electronic devices.

8.9 Security arrangements will be reviewed regularly, any reported breaches or potential weaknesses will be investigated and, where necessary, further or alternative measures will be introduced to secure the data.

8.10 Employees who process personal data out of the Trust (e.g. on another site, at home) can only do this with the express consent of their Headteacher / line manager. In the case of teaching staff it is recognised that pupil workbooks etc may be taken home regularly for assessment purposes. Such materials must be kept securely at home and whilst in transit. Sensitive personal data must never be removed from the workplace.

8.11 Access to personal data outside of the Trust should not be attempted using unsecured access systems (this includes via mobile networks outside of UK unless the network has been checked in advance to be compliant under data protection law).

8.12 System testing will only be carried out using personal data where sufficient safeguards are in place and will not be undertaken on live databases accessing live personal sensitive data.

8.13 Personal data will not be transferred outside the European Economic Area without the approval of the data controller.

8.14 Wherever possible, personal data should not be shared with governors and Trustees unless absolutely necessary for the purposes of governance. Such data will only be stored in the Governors Virtual Office (GVO) or its successor secure system and will not be attached to email.

8.15 Minutes and other records of meetings, where they contain personal data, will only be stored in the GVO or other secure Trust system. No personal data will be included in minutes or other records of meetings which are published on Trust websites.

9. Data Subject Rights

The Trust will comply with its obligations under current data protection regulation in this regard. Please refer to the separate Subject Access Requests Policy.

10. Disclosure and Sharing

10.1 Third party access to information

10.1.1 Where a request for personal data is made by a third party on behalf of the data subject it shall be treated as a subject access request. Evidence is required that the third party is entitled to act in this way, such as a written statement from the data subject or an enduring power of attorney. Appropriate professionals may need to be consulted before a decision to release the personal data is made.

10.1.2 Occasionally third party information may form part of the data extracted in response to a subject access request. In deciding whether to release this information, the Trust will consider the following:

- any duty of confidentiality owed to the third party;
- attempts to get consent from the third party;
- any express refusal of consent from the third party;
- the third party's expectations with respect to that data.

10.1.3 When a request for personal data is made by a third party and not on behalf of the data subject, the Trust shall consider the request under Freedom of Information as well as GDPR. It shall consider whether releasing the personal data would breach any of the Data Protection principles and in particular whether any exemptions under GDPR apply. Personal information will not be shared with third parties unless specifically allowed for in law and justified in the specific situation.

10.1.4 The Freedom of Information policy deals with requests for information about third parties, and information will be withheld where disclosing it would breach any of the Data Protection principles. Where a requester does not state a specific reason for requesting the information then the FOI policy should be followed. A response to an FOI request must not take into account the reasons behind the request.

10.1.5 When there is a specific reason for requesting the information, an exemption under GDPR may apply. Examples are where information is required for the prevention or detection of crime, apprehension or prosecution of offenders or assessment or collection of tax.

10.1.6 If an appropriate exemption under GDPR does apply so that the Data Protection principles will not be breached, the Trust will usually comply with the request. However, without a Court Order there is no obligation on the Trust to disclose the information.

10.1.7 Where the Trust is not convinced that the third party has entitlement to the personal data, or that any exemptions under GDPR apply, and that releasing information would breach the Data Protection principles, the personal data will be withheld and only released on presentation of a Court Order.

10.2 Information sharing

10.2.1 The Trust promotes information sharing where it is in the best interests of the data subject. However, personal sensitive data will not be shared unless it is in connection with the primary purpose for which the information was collected, or the data subject has explicitly given their permission for the information to be shared for this purpose, or another legal provision (GDPR exemption exists) to allow the sharing such information.

10.2.2 The Trust will ensure that supporting processes and documentation are made available to professionals so that they understand how to share information safely and lawfully.

10.2.3 Where an employee acting in good faith has shared information in accordance with these supporting processes and documentation, they shall not normally be subject to disciplinary action under section 5.2, hereof.

10.2.4 Sharing large sets of information, or recurrent regular sharing shall be carried out under written agreement to ensure the continued compliance with the GDPR and that additional safeguards can be considered and put in place.

10.3 Contractual and partnership arrangements

10.3.1 When the Trust enters contractual or partnership arrangements which involve the processing of personal data, a written agreement will specify which party is data controller or whether there are joint data controller arrangements. Where a third party is processing personal data and information on behalf of the Trust, a written contract will be put in place. Specific care will be taken in respect of services provided online and via 'the cloud'.

10.3.2 Where the Trust remains as data controller, it will take steps to ensure that the processing by its contractors and sub-contractors will comply with GDPR. Contractors will not be able to sub-contract Data Processing without the explicit written permission of the Trust. Staff will take reasonable steps to ensure that data processing by third parties is regularly monitored to ensure GDPR requirements are being met.

10.3.3 Where the parties are data controllers jointly or in common, the Trust will liaise with the other party to ensure that all processing complies with GDPR. The responsibilities of each data controller should be expressly and clearly laid out.

10.3.4 All contractors who are users of personal information supplied by the Trust will be required to confirm that they will abide by the requirements of the Regulation to the same standard as the Trust with regard to information supplied by the Trust. Staff should obtain advice from Legal Services as necessary.

10.3.5 All contractors, consultants, partners or agents of the Trust must ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the Trust, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Regulation. Any breach of any provision of the Regulation will be deemed as being a breach of the contract between the Trust and that individual, company, partner or firm. The Trust shall take reasonable

steps to ensure regular monitoring of contracts and specifically the security of data being processed on its behalf.

10.3.6 Any observed or suspected security incidents or security concerns should be reported to the Trust.

10.3.7 All contractors, consultants, partners or agents of the Trust must allow data protection audits by the Trust of data held on its behalf if requested in line with these contractual arrangements.

10.3.8 All contractors, consultants, partners or agents of the Trust must indemnify the Trust against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

11. Avoiding data breaches

11.1 The possibility that confidential information may be viewed on a screen by unauthorised persons must be considered when positioning devices in a classroom or office space.

11.2 Staff must be careful not to display confidential information using a digital projector or other teachers' wall display unit.

11.3 When printing or photocopying any confidential data, the device or printer must be physically secure or attended. The use of FollowMe printing provides this security.

11.4 Email addresses and fax numbers should be checked carefully prior to dispatch, especially where the information content constitutes personal, and especially sensitive personal data.

12. Registration with the ICO

12.1 The Trust has a notification registered with the Information Commissioner under registration number ZA161410.

12.2 The Business Director will ensure that this notification is an accurate description of processing carried out by the Trust.

12.3 The Trust is responsible for submitting this notification to the Information Commissioner.

12.4 When the Trust plans to carry out new processing not covered by this notification, it will amend the notification (if necessary) within 28 days of processing beginning.

13. Subject Access Requests and Data Protection Complaints

For information on the how the Trust deals with Subject access requests please refer to the Subject Access Requests Policy.

Data protection complaints should be addressed to the Business Director at enquiries@wellswaymat.com

Complaints about the Trust's processing of personal data and rights under the General Data Protection Regulation will be dealt with in accordance with this Policy and associated Trust policies. Complaints will be fully dealt with after a formal review.

Individuals have a right to request that the Information Commissioner make an assessment of compliance of particular circumstances with the General Data Protection Regulation. If

individuals are not happy about how the Trust has handled their information they can contact the ICO via the following means:

By post to:
Customer Contact
Information Commissioner's Office,
Wycliffe House,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF

Alternatively visit their website - www.ico.gov.uk or contact them by phone on 0303 1231113.

The Trust will respond promptly and fully to any request for information about data protection compliance made by the Information Commissioner.

The Trust will comply with any Information Commissioner Information Notice (to provide answers and information to the Commissioner) or Enforcement Notice (for failure to provide answers or information or for a breach of the Act) sent to the Trust by the Information Commissioner. The Commissioner can also carry out audits, prosecute individuals and organisations and report concerns to parliament.

14. Implementation

14.1 The responsibility for implementation of this policy rests with the Trust.

14.2 The Trust will ensure that:

- Everyone managing and/or handling personal information understands that they are contractually responsible for following good data protection practice.
- Everyone managing and/or handling personal information is appropriately trained to do so.
- Everyone managing and/or handling personal information is appropriately supervised.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, is given advice as necessary.
- Queries about handling personal information are promptly and courteously dealt with.
- Methods of handling personal information are regularly assessed and evaluated.
- Performance with handling personal information is regularly assessed and evaluated.
- Employees are aware of the action required in the event of a Data Breach.

14.3 On joining the Trust, employees are required to undertake training on Data Protection and IT Security as part of their induction.

14.4 The Data Protection Officer works with the Trust to maintain the on-going programme of annual training and awareness to maintain a high level of understanding of Data Protection and security among all staff and to communicate any legal or policy changes that occur.

14.5 Data Protection audits are regularly carried out by internal audit (external audits may be commissioned if required) in order to monitor compliance with the GDPR and this policy.

14.6 The Trust Audit & Risk Committee will receive an annual report on data governance generally; this will also include details of any data breaches.

15. Other related policies

This policy should be interpreted and applied in relation to other related policies. Breach of these policies will automatically breach this policy and this is likely to contravene the General Data Protection Regulation and other legislation. These related policies include, but are not limited to, the following and such other policies as are adopted by the Trust from time to time:

IT Security Policy
Freedom of Information Policy
The Safer Working Practice Policy
Subject Access Policy
CCTV Policy