



# Wellsway Multi Academy Trust Data Protection Policy

## 1. INTRODUCTION

- 1.1. Wellsway Multi Academy Trust (WMAT) collects and uses certain types of personal information about staff, pupils, parents and other individuals who come into contact with the Trust in order to provide education and associated functions. The Trust may be required by law to collect and use certain types of information to comply with statutory obligations related to employment, education and safeguarding, and this policy is intended to ensure that personal information is dealt with properly and securely and in accordance with the Data Protection Act 1998 ("the DPA") and other related legislation. It will apply to information regardless of the way it is used, recorded and applies for as long as the information is held.
- 1.2. This policy will be updated as necessary to reflect best practice, or amendments made to the DPA, and shall be reviewed every two years.

## 2. PERSONAL DATA

- 2.1. 'Personal data' is information that identifies an individual, and includes information that would identify an individual to the person to whom it is disclosed because of any special knowledge that they have or can obtain<sup>1</sup>. A sub-set of personal data is known as 'sensitive personal data'. Sensitive personal data is information relating to race or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, trade union membership, physical or mental health, sexual life or the commission of any offence. Sensitive personal data is given special protection.
- 2.2. The Trust does not intend to seek or hold sensitive personal data about staff or students except where the Trust has been notified of the information, or it comes to the Trust's

---

<sup>1</sup> For example, if asked for the number of female employees, and you only have one female employee, this would be personal data if it was possible to obtain a list of employees from the website.

attention via legitimate means (e.g. a grievance) or needs to be sought and held in compliance with a legal obligation or as a matter of good practice. Staff or students are under no obligation to disclose to the Trust their race or ethnic origin, political or religious beliefs, whether or not they are a trade union member or details of their sexual life (save to the extent that details of marital status and/or parenthood are needed for other purposes, e.g. pension entitlements).

### **3. THE DATA PROTECTION PRINCIPLES**

3.1. The eight data protection principles as laid down in the DPA are followed at all times:

- (1) Data must be processed fairly and lawfully, and only where one of the conditions in Schedule 2 DPA can be met. If sensitive personal data, a condition in Schedule 3 DPA must also be met;
- (2) Personal data shall be obtained only for one or more specific and lawful purposes;
- (3) Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed;
- (4) Personal data shall be accurate and where necessary kept up to date;
- (5) Personal data processed for any purpose(s) shall not be kept for longer than is necessary for that purpose/those purposes;
- (6) Personal data shall be processed in accordance with the rights of data subjects under the DPA;
- (7) 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;
- (8) Personal data shall not be transferred to a country outside the EEA, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data;

3.2 The Trust is committed to maintaining those principles at all times. This means that the Trust will:

- 3.2.1 Inform parents, staff and others as to the purpose of collecting any information from them, as and when we ask for it;
- 3.2.2 Be responsible for checking the quality and accuracy of the information;
- 3.2.3 Regularly review the records held to ensure that information is not held longer than is necessary [and that it has been held in accordance with the data retention policy];
- 3.2.4 Ensure that when information is authorised for disposal it is done appropriately;
- 3.2.5 Ensure appropriate security measures to safeguard personal information whether it is held in paper files or on our computer system;

- 3.2.6 Share personal information with others only when it is necessary and legally appropriate to do so, ensuring that pupil names are replaced with unique pupil numbers in records before data is transferred where appropriate;
- 3.2.7 Set out clear procedures for responding to requests for access to personal information known as subject access in the DPA;
- 3.2.8 Report any breaches of the DPA as soon as they occur, or in any event within 24 hours of the breach coming to the Trust's attention. Breaches should be notified to the Business Director in the first instance, who will then decide what action, if any, needs to be taken.

#### **4 BREACH OF ANY REQUIREMENT OF THE DPA**

- 4.1 Any and all breaches of the DPA, including a breach of any of the data protection principles, shall be reported as set out in paragraph 3.2.8 above.
- 4.2 Once notified, the Business Director shall assess the extent of the breach, and the potential consequences, and decide whether notification to the Information Commissioner's Office (ICO) and/or the Charity Commission is necessary.
- 4.3 The Business Director shall then be responsible for instigating an investigation into the breach, including how it happened, and whether it could have been prevented. Any recommendations for further training or a change in procedure shall be reviewed by the governors and a decision made about implementation of those recommendations.

#### **5 USE OF PERSONAL DATA BY THE TRUST**

- 5.1 The Trust holds personal data on pupils, staff and other individuals such as visitors. In each case, the personal data must be treated in accordance with the data protection principles as outlined in paragraph 3.1 above.

##### **Pupils**

- 5.2 The personal data held regarding pupils includes contact details, assessment/examination results, attendance information, characteristics such as ethnic group, special educational needs, any relevant medical information, and photographs.
- 5.3 The data is used in order to support the education of the pupils, to monitor and report on their progress, to provide appropriate pastoral care, and to assess how well the Trust as a whole is doing, together with any other uses normally associated with this provision in an independent school environment.
- 5.4 The Trust may make use of limited personal data (such as contact details) relating to pupils, and their parents or guardians for fundraising, marketing or promotional purposes and to maintain relationships with pupils of the Trust, but only where consent has been provided to this.
- 5.5 In particular, the Trust may:

- 5.5.1 transfer information to any association society or club set up for the purpose of maintaining contact with pupils or for fundraising, marketing or promotional purposes relating to the academy;
- 5.5.2 make use of photographs of pupils in Trust publications and on the Trust websites;
- 5.5.3 disclose photographs and names of pupils to the media (or allow the media to take photographs of pupils) for promotional and congratulatory purposes where a pupil may be identified by name when the photograph is published e.g. where a pupil has won an award or has otherwise excelled;
- 5.5.4 make personal data, including sensitive personal data, available to staff for planning curricular or extra-curricular activities;
- 5.5.5 keep the pupil's previous school informed of his/her academic progress and achievements e.g. sending a copy of the school reports for the pupil's first year at the Trust to their previous school.

5.6 Photographs with names identifying pupils will not be published on Trust websites without the express permission of the appropriate individual.

5.7 Any wish to limit or object to any use of personal data should be notified to the school Headteacher in writing, which notice will be acknowledged by the school in writing. If, in the view of Headteacher, the objection cannot be maintained, the individual will be given written reasons why the school cannot comply with their request. Parents who do not want their child's photograph or image to appear in any of the Trust's promotional material, or be otherwise published, must also make sure their child knows this.

5.8 Pupils, parents and guardians should be aware that where photographs or other image recordings are taken by family members or friends for personal use the DPA will not apply e.g. where a parent takes a photograph of their child and some friends taking part in the School sports day.

#### **Staff**

5.9 The personal data held about staff will include contact details, employment history, information relating to career progression, information relating to DBS checks, photographs.

5.10 The data is used to comply with legal obligations placed on the Trust in relation to employment, and the education of children in a school environment. The Trust may pass information to other regulatory authorities where appropriate, and may use names and photographs of staff in publicity and promotional material. Personal data will also be used when giving references.

5.11 Staff should note that information about disciplinary action may be kept for longer than the duration of the sanction. Although treated as "spent" once the period of the sanction has expired, the details of the incident may need to be kept for a longer period.

5.12 Any wish to limit or object to the uses to which personal data is to be put should be notified to the HR Manager who will ensure that this is recorded, and adhered to if appropriate. If the HR Manager is of the view that it is not appropriate to limit the use of personal data in the way

specified, the individual will be given written reasons why the Trust cannot comply with their request.

### **Other Individuals**

5.13 The Trust may hold personal information in relation to other individuals who have contact with the school, such as volunteers and guests. Such information shall be held only in accordance with the data protection principles, and shall not be kept longer than necessary.

## **6 SECURITY OF PERSONAL DATA**

6.1 The Trust will take reasonable steps to ensure that members of staff will only have access to personal data relating to pupils, their parents or guardians where it is necessary for them to do so. All staff will be made aware of this Policy and their duties under the DPA. The Trust will take all reasonable steps to ensure that all personal information is held securely and is not accessible to unauthorised persons.

## **7 DISCLOSURE OF PERSONAL DATA TO THIRD PARTIES**

7.1 The following list includes the most usual reasons that the Trust will authorise disclosure of personal data to a third party:

- 7.1.1 To give a confidential reference relating to a current or former employee, volunteer or pupil;
- 7.1.2 for the prevention or detection of crime;
- 7.1.3 for the assessment of any tax or duty;
- 7.1.4 where it is necessary to exercise a right or obligation conferred or imposed by law upon the Trust (other than an obligation imposed by contract);
- 7.1.5 for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings);
- 7.1.6 for the purpose of obtaining legal advice;
- 7.1.7 for research, historical and statistical purposes (so long as this neither supports decisions in relation to individuals, nor causes substantial damage or distress);
- 7.1.8 to publish the results of public examinations or other achievements of pupils of the Trust;
- 7.1.9 to disclose details of a pupil's medical condition where it is in the pupil's interests to do so, for example for medical advice, insurance purposes or to organisers of school trips;

7.1.10 to provide information to another educational establishment to which a pupil is transferring;

7.1.11 to provide information to the Examination Authority as part of the examination process; and

7.1.12 to provide information to the relevant Government Department concerned with national education. At the time of the writing of this Policy, the Government Department concerned with national education is the Department for Education (DfE). The Examination Authority may also pass information to the DfE.

7.2 The DfE uses information about pupils for statistical purposes, to evaluate and develop education policy and to monitor the performance of the nation's education service as a whole. The statistics are used in such a way that individual pupils cannot be identified from them. On occasion the DfE may share the personal data with other Government Departments or agencies strictly for statistical or research purposes.

7.3 The Trust may receive requests from third parties (i.e. those other than the data subject, the Trust, and employees of the Trust) to disclose personal data it holds about pupils, their parents or guardians, staff or other individuals. This information will not generally be disclosed unless one of the specific exemptions under the DPA which allow disclosure applies; or where necessary for the legitimate interests of the individual concerned or the Trust.

7.4 All requests for the disclosure of personal data must be sent to Business Director, who will review and decide whether to make the disclosure, ensuring that reasonable steps are taken to verify the identity of that third party before making any disclosure.

## **8 CONFIDENTIALITY OF PUPIL CONCERNS**

8.1 Where a pupil seeks to raise concerns confidentially with a member of staff and expressly withholds their agreement to their personal data being disclosed to their parents or guardian, the Trust will maintain confidentiality unless it has reasonable grounds to believe that the pupil does not fully understand the consequences of withholding their consent, or where the Trust believes disclosure will be in the best interests of the pupil or other pupils.

## **9 DEALING WITH A SUBJECT ACCESS REQUEST**

9.1 Anybody who makes a request to see their file or their child's file or other personal data held on them is making a subject access request under the DPA. All information relating to the individual, including that held in day books, diaries and on electronic systems and email should be considered for disclosure.

9.2 All requests must be dealt with within 40 days of receipt – regardless of any school holidays.

9.3 Where a child or young person does not have sufficient understanding to make his or her own request (usually those under the age of 12, or over 12 but with a special educational need

which makes understanding their information rights more difficult), a person with parental responsibility can make a request on their behalf. The Headteacher must, however, be satisfied that:

9.3.1 the child or young person lacks sufficient understanding; and

9.3.2 the request made on behalf of the child or young person is in their interests.

9.4 The Trust will only grant pupils' access to their personal data if, in the Trust's reasonable belief, the pupil understands the nature of the request.

9.5 Any individual, including a child or young person with ownership of their own information rights may appoint another person to request access to their records. In such circumstances the Trust must have written evidence that the individual has authorised the person to make the application and the Headteacher must be confident of the identity of the individual making the request and of the authorisation of the individual to whom the request relates.

9.6 Access to records will be refused in instances where an exemption in the DPA applies, for example, information sharing may place a child at risk of significant harm or jeopardise police investigations into any alleged offence(s).

9.7 A subject access request under the DPA must be made in writing and the Trust must respond within 40 days. The Trust may ask for any further information reasonably required to locate the information.

9.8 An individual only has the automatic right to access information about themselves, and care needs to be taken not to disclose the personal data of third parties where you do not have their consent, or where seeking consent would not be reasonable, and it would not be appropriate to release the information.

9.9 All files must be reviewed by Headteacher before any disclosure takes place. Access will not be granted before this review has taken place.

9.10 Where all the data in a document cannot be disclosed, a permanent copy should be made and the data obscured retyped if this is more sensible. A copy of the full document and the altered document should be retained, with the reason why the document was altered.

9.11 If an individual discovers that information which the Trust holds in relation to them is inaccurate or out of date, they should write to Headteacher setting out the inaccuracy, and the accurate position. The Headteacher will arrange for information to be corrected where the Trust is in agreement that the previous information was inaccurate. If the Trust disagrees that the information is inaccurate, it will discuss the matter with the individual, but the Trust has the right to maintain the original information. If the individual is unhappy with this outcome [they have the right to instigate the complaints procedure/request a review of the decision by a governor, as long as such review is requested with [30] days of the date of receipt of the letter, and this deadline has been notified to the individual in correspondence].

#### **Exemptions to Access by Data Subjects**

9.12 Confidential references given, or to be given by the Trust, are exempt from subject access. The Trust will therefore treat as exempt any reference given by them for the purpose of the

education, training or employment, or prospective education, training or employment of any pupil, member of staff, or volunteer.

9.13 It should be noted that confidential references received from other parties may also be exempt from disclosure, under the common law of confidence. However, such a reference can be disclosed if such disclosure will not identify the source of the reference or where, notwithstanding this, the referee has given their consent, or where disclosure is reasonable in all the circumstances.

9.14 Examination scripts, i.e. information recorded by pupils during an examination, are exempt from disclosure. However, any comments recorded by the examiner in the margins of the script are not exempt even though they may not seem of much value without the script itself.

9.15 Examination marks do not fall within an exemption as such. However, the 40 day compliance period for responding to a request is extended in relation to examination marks to either five months from the day on which the Trust received the request or 40 days from the announcement of the examination results, whichever is the earlier.

9.16 Where a claim to legal professional privilege could be maintained in legal proceedings, the information is exempt from disclosure unless the privilege is waived.

#### **Repeated Requests for Access to Records**

9.17 Unless a reasonable period of time has lapsed between the compliance with one request and receipt of the next, the DPA allows for access to be refused when the applicant has made repeated requests for information already provided.

#### **Charging**

9.18 The maximum fee which can be charged is £10 and must not exceed the cost of supplying the information. The Academy does not intend to charge this fee as a matter of course, and this is made clear on the website.

#### **Section 10 Notices**

9.19 Any request to stop dealing with personal data by the Trust because of damage or distress caused should be treated as a request under section 10 DPA. Any such request must be notified to Business Director, who will deal with them as appropriate.

Throughout section 9, where reference is made to 'Headteacher' this should be replaced by 'Business Director' where staff who are not employed at any specific school are concerned.

## **10 STAFF PROCEDURES AND TRAINING**

WMAT will ensure that:

- All staff are aware of their responsibilities under the Data Protection Act.
- All staff are aware of their responsibilities under the Data Retention Regulations.
- Staff are trained and supported to deal effectively with the requirements of the Act, including the need to deal with subject access requests, in whole or in part, in accordance with the Act.



Training will be deployed as follows:

<b>User Group</b>	<b>Main areas of procedure</b>	<b>Training</b>
Headteachers and senior leaders	Dealing with subject access requests Use of surveillance eg CCTV Storing and disposal of hard and soft personal data Use of biometrics Taking and using photographs	Annually, overview of key elements of DPA and WMAT procedures
Audit & Risk Committee members		Annually, overview of key elements of DPA and WMAT procedures
Reception and admin staff	Dealing with subject access requests Storing and releasing references Use of biometrics	Annually, overview of WMAT procedures including data disposal and other department specific procedures
Premises team	Use of surveillance eg CCTV	Annually, overview of WMAT procedures including data disposal and other department specific procedures
IT Team	Disposal of soft student and staff data Security of IT systems Use of biometrics Acceptable use of IT Use of cloud based software	Annually, overview of WMAT procedures including data disposal and other department specific procedures
Business / marketing staff	Use of direct marketing Use of photographs of children	Annually, overview of WMAT procedures including data disposal and other department specific procedures
Other staff		Not required, access to policy by all staff

Training guidelines for schools can be found at <https://ico.org.uk/for-organisations/education/>

**This policy should be read in conjunction with the IT Security Policy which covers:**

- **back up**
- **endpoint protection (patching, anti-virus etc)**
- **email retention**
- **password policy**
- **device encryption**
- **bring your own device policy**