

Privacy Notice: Workforce (Staff)

2024-25

Date approved:	16.9.24
Approved by:	CFO
Date adopted by the MAT (i.e. effective date):	September 2024
This policy is scheduled for review on:	Annually

Contents

Policy Statement	3
Scope	3
How we use workforce information.....	4
Why we collect and use workforce information	5
Information Requests	8
Collecting workforce information	8
Storing workforce information.....	8
Who we share workforce information with	9
Why we share school workforce information	10
Local authority	10
Department for Education (DfE).....	10
Requesting access to your personal data	10
How Government uses your data	11
Data collection requirements.....	11
Sharing by the DfE.....	11
Contact.....	12
Breach of Policy.....	13

Policy Statement

This policy outlines Manor Multi Academy Trust's ('we' / 'our' / 'us') expectations in relation to use of staff personal data.

We are committed to equality and value diversity. As such we are committed to fulfilling our Public Sector Equality Duty (Equality Duty) obligations and expect all staff and volunteers to share this commitment.

This policy should also be applied in accordance with our Staff Code of Conduct, Dignity at Work, Safeguarding and Child Protection, Safer Recruitment, and ICT Acceptable Use policies and Procedures. Copies of all policies and procedures can be accessed via the **All MAT Staff** area on Teams.

The Equality Duty requires us to have due regard to the need to:

- Eliminate unlawful discrimination, harassment, and victimisation.
- Advance equality of opportunity.
- Foster good relations between people who share protected characteristics, such as age, gender, race and faith, and people who do not share them.

If you consider that any of our practices, policies or procedures may be indirectly discriminatory, you should report your concerns and the basis for them to your line manager, who will take appropriate action and ensure that you receive a written response in respect of the concerns that you have raised.

This policy does not form part of your contract of employment. We reserve the right to amend or withdraw this policy at any time.

We are responsible for ensuring the effective implementation of this policy. As part of equality monitoring we will review and monitor the operation and impact of the policy on a regular basis and in accordance with the policy review date. As part of this monitoring and review this policy will be equality impact assessed.

Scope

This policy applies to employees, workers, agency workers, consultants, casual workers, contractors and volunteers, whether during working hours or otherwise.

This Policy provides information which underpins our Staff Code of Conduct, and Disciplinary Policy and Procedures. Copies of these policies and procedures can be accessed via the **All MAT Staff** area on Teams.

How we use workforce information

We are committed to providing a secure and safeguarded environment for all our workforce. Security of all data and personal information is of paramount importance and we strongly believe that each and every employee has a duty of care to ensure all personal data is treated with upmost respect and care. It is strongly advised that all staff read this privacy notice carefully as well as the associated Data Protection, Safeguarding and Child Protection and e-Safety Policies that encompass our true reflection on our approach to all aspects of operating our secure environment.

It is also very important that you understand that the use of any personal data will be lawfully processed and used for multiple work-related purposes during the term of your employment with us. We encourage you to question this if you feel this may not be the case and to bring to the immediate attention of our Data Protection Officer.

The categories of information that we process include:

- personal information (such as name, employee or teacher number, national insurance number)
- characteristics information (such as gender, age, ethnic group)
- contract information (such as start date, hours worked, post, roles and salary information)
- work absence information (such as number of absences and reasons)
- qualifications (and, where relevant, subjects taught)
- photographs
- education details
- employment details
- financial details
- absence and holiday records
- disciplinary and grievance records
- CPD information (training record)
- relevant medical and dietary information, including Doctors' details
- DBS (Disclosure & Barring Service) – may include Passport, Utility Bills, Driving License information
- emergency contact details (Name and contact number) of spouse, partner or family members

This list is not exhaustive but covers the majority of personal details we may process and hold on record during the time of your employment.

Why we collect and use workforce information

We use workforce data to:

- a) enable the development of a comprehensive picture of the workforce and how it is deployed
- b) inform the development of recruitment and retention policies
- c) enable individuals to be paid
- d) to administer school property
- e) to maintain our own accounts and records
- f) to carry out fundraising
- g) to support staff CPD & training
- h) to provide appropriate pastoral care
- i) to assess the quality of our provision
- j) to comply with the law regarding data sharing

Under the UK General Data Protection Regulation (UK GDPR), the legal basis we rely on for processing personal information for general purposes are (Article 6):

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
 - a. the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
 - b. 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;
 - c. processing is necessary for compliance with a legal obligation to which the controller is subject;
 - d. processing is necessary in order to protect the vital interests of the data subject or of another natural person;
 - e. 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;
 - f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing

procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations.

2. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
 - any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
 - the context in which the personal data has been collected, in particular regarding the relationship between data subjects and the controller;
 - the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
 - the possible consequences of the intended further processing for data subjects;
 - the existence of appropriate safeguards, which may include encryption or pseudonymisation.

In addition, concerning any special category data (Article 9):

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
 - a. the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
 - b. processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by law or a collective agreement pursuant to law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
 - c. processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - d. processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former

members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

- e. processing relates to personal data which are manifestly made public by the data subject;
 - f. processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
 - g. processing is necessary for reasons of substantial public interest, on the basis of law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
 - h. processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
 - i. processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
 - j. processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89\(1\)](#) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under law or rules established by national competent bodies.
 4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Information Requests

Exemptions and Confidential References:

Under the UK General Data Protection Regulation (GDPR) and the Data Protection Act 2018, there are exemptions that allow organisations like ours to withhold certain information in specific circumstances. These exemptions are not a “one size fits all” solution; rather, they need to be considered on a case-by-case basis.

1. Why Exemptions Matter:
 - The UK GDPR and the Data Protection Act 2018 outline exemptions from various rights and obligations related to personal data processing.
 - An exemption often depends on the purpose for which you process personal data.
2. What Are Exemptions?
 - The DPA 2018 provides several exemptions, detailed in [Schedules 2-4](#).
 - Exemptions such as the right to be informed, the right of access, and dealing with other individual rights.
 - Some exemptions apply to specific aspects, while others can exempt our organisation from multiple requirements.
3. Confidential Employment References:
 - Schedule 2 of the Data Protection Act 2018 gives employers an exemption for “confidential employment references.”
 - What does this mean? As an employer, we can withhold certain employment references without violating data protection rules.

As an education organisation we MUST use **Safeguarding** as a strict exemption if we feel releasing personal information under any request could put any child, family members or employee associated with the request at risk. This also includes whether redactions have been made for any information, this would still be considered a risk.

Collecting workforce information

We may collect personal information via electronic or manual handwritten form method.

Workforce data is essential for our and the Local Authority’s operational use. Whilst the majority of personal information you provide to us is mandatory, some of it is requested on a voluntary basis. In order to comply with GDPR, we will inform you at the point of collection, whether you are required to provide certain information to us or if you have a choice in this.

Storing workforce information

We hold data securely at Manor Multi Academy Trust and our Schools will retain workforce information during the employment of the individual and thereafter for the recommended retention period legally required. . Workforce information can be stored in two secure ways.

1. Limited manual records will be kept in a secure room within secure locked filing cabinets. Physical access to the storage is limited by key or secure monitored door access.
2. Electronically the information is securely stored on cloud infrastructure on an encrypted physical drive which is also permissioned and account password protected accordingly to staff that only require access to this information. Administrative ICT access is allowed for maintenance reasons including backup and retention. It is also required to remove the information as and when the retention schedule on the data ends. Cloud based backup location remain with the Multi Academy Trust and not shared with any 3rd Party. All 3rd Party agreements and privacy policies or data security information are kept and updated as required. Information is secured within Manor Multi Academy Trust Microsoft Office 365 cloud environment, again this is account password protected and permissioned accordingly. The Trust configuration determines that all information synchronised / stored on devices are account / password or pin protected as well as being encrypted if Windows based. Mobile devices require a minimum of pin code or password protection which are not to be shared.

Who we share workforce information with

We may need to or routinely share this information with:

- Associated Local Authorities representative to the which the location of the School in the Trust resides
- The Department for Education (DfE) and central government
- Education, training, careers and examining bodies
- School / Trust MIS systems and other online subscriptions
- School staff, PCAF representatives and Directors
- Family, associates and representatives of the person whose personal data we are processing
- Financial organisations and systems we use such as Payroll
- NHS and healthcare professionals
- Social and welfare organisations
- Law enforcement organisation, solicitors and courts
- Current, past or prospective employers
- Trust business associates (including all schools)
- Professional advisers (i.e Legal, Social Care, Coaching, NHS and Police)
- Suppliers and service providers (E.g. HR & Payroll)
- Financial organisations
- Security organisations (including CCTV and signing in systems)
- Press and the media
- School trip organisations

The above list is not exhaustive but includes current working practises and the potential for information to be shared with legally, appropriately and purposefully in the interest of all parties involved.

Why we share school workforce information

We do not share information about our workforce members with anyone without consent unless the law and our policies allow us to do so.

Local authority

We are required to share information about our workforce members with our Local Authority (LA) under Section 5 of the Education (Supply of Information about the School Workforce) (England) Regulations 2007 and amendments.

Department for Education (DfE)

The DfE collects personal data from educational settings and LA's via various statutory data collections. We are required to share information about our children and young people with the DfE for the purpose of those data collections, in accordance with the Data Protection Act 1998.

The DfE has legal powers to collect the pupil, child and workforce data that schools, local authorities and awarding bodies hold.

For more information on the legislation which allows this, see:

- [section 114 of the Education Act 2005](#)
- [section 537A of the Education Act 1996](#)
- [section 83 of the Children Act 1989](#)

This data forms a significant part of our evidence base. We use it:

- in school performance tables
- in adoption scorecards
- in statistical first releases
- to evaluate and inform educational policy
- to assess funding to local authorities and schools

All data is transferred securely and held by DfE under a combination of software and hardware controls which meet the current [government security policy framework](#).

For more information, please see 'How Government uses your data' section.

Requesting access to your personal data

Under data protection legislation, you have the right to request access to information about you that we hold. To make a request for your personal information, contact our Data Protection Officer dpo@manormat.com.

You also have the right to:

- to ask us for access to information about you that we hold
- to have your personal data rectified, if it is inaccurate or incomplete
- to request the deletion or removal of personal data where there is no compelling reason for its continued processing
- to restrict our processing of your personal data (i.e. permitting its storage but no further processing)
- object to processing of personal data that is likely to cause, or is causing, damage or distress
- prevent processing for the purpose of direct marketing
- object to decisions being taken by automated means
- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- a right to seek redress, either through the ICO, or through the courts

It is your co-responsibility to ensure the information we hold is up to date and accurate. This should be in writing to the Trust / School office so this can be updated accordingly.

If you have a concern about the way we are collecting or using your personal data, we ask that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at <https://ico.org.uk/concerns/>

How Government uses your data

The workforce data that we lawfully share with the DfE through data collections:

- informs departmental policy on pay and the monitoring of the effectiveness and diversity of the school workforce
- links to school funding and expenditure
- supports 'longer term' research and monitoring of educational policy

Data collection requirements

To find out more about the data collection requirements placed on us by the Department for Education including the data that we share with them, go to <https://www.gov.uk/education/data-collection-and-censuses-for-schools>.

Sharing by the DfE

The Department may share information about school employees with third parties who promote the education or well-being of children or the effective deployment of school staff in England by:

- conducting research or analysis

- producing statistics
- providing information, advice or guidance

The Department has robust processes in place to ensure that the confidentiality of personal data is maintained and there are stringent controls in place regarding access to it and its use. Decisions on whether the DfE releases personal data to third parties are subject to a strict approval process and based on a detailed assessment of:

- who is requesting the data
- the purpose for which it is required
- the level and sensitivity of data requested; and
- the arrangements in place to securely store and handle the data

To be granted access to school workforce information, organisations must comply with its strict terms and conditions covering the confidentiality and handling of the data, security arrangements and retention and use of the data.

To contact the Department: <https://www.gov.uk/contact-dfe>

Contact

If you would like to discuss anything in this privacy notice, please contact:

If you would like to get any further clarification of the information about you that Manor Multi Academy Trust (Manor Primary School) shares with the DfE or how they use your information, please contact:

Name: Neil Beards

Email: dpo@manormat.com

Address: Manor Multi Academy Trust
Ettingshall Road
Wolverhampton
West Midlands
WV14 9UQ

Telephone: 01902 556460

Website: <http://www.manormat.com>

To contact the DfE, please visit: <https://www.gov.uk/contact-dfe>

Breach of Policy

Any breaches of this procedure by staff will be managed under the Trust's Disciplinary Policy and Procedure, which can be located in the **All MAT Staff** area on Teams.