



Privacy Notice for Job Applicants, Employees, Students, Trustees and Volunteers

Purpose of this document

As an employer, Manchester Settlement must meet its contractual, statutory and administrative obligations. We are committed to protecting the privacy and security of your personal information and ensuring that your personal data is handled in accordance with the principles set out in Data Protection Act 2018.

Manchester Settlement is a “data controller”. This means that we are responsible for deciding how we hold and use personal information about You. We are required under data protection legislation to notify You of the information contained in this privacy notice.

It is important that you read this document, so that you are aware of how and why we are using your personal information and the rights you have in relation to your personal information.

This privacy notice applies to all job applicants, employees, students, volunteers and trustees. However, the information we will process about you will vary depending on your specific role and personal circumstances.

This document should be read in conjunction with our Data Protection Policy.

The kind of information we hold about you and why

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). There are “special categories” of more sensitive personal data which require a higher level of protection, such as information about a person’s beliefs, ethnic origin, health or sexual orientation.

Information related to your job or volunteering application

We process the following types of personal information:

- Personal contact details such as your name, address, telephone and personal email addresses
- Information about your employment and education history including your qualifications, CV or job application, any dismissals or references
- Evidence of your right to work in the UK or your immigration status

We use this information to:

- Carry out our recruitment process such as progressing your applications, making an informed decision to shortlist for interview or appoint the best candidate for the role, provide and demonstrate a fair and reasonable recruitment process
- Fulfil our legal obligations where we are required to satisfy ourselves that you have the right to work in the UK under the Immigration, Asylum and Nationality Act 2006

Information related to your employment or contractual relationship with us

We process the following types of personal information:

- Personal contact details such as your name, address, telephone and personal email addresses
- Your date of birth, gender and NI number

- A copy of your passport or similar photographic identification and /or proof of address documents such as your driving licence
- Next of kin, emergency contacts and their contact information
- Details of any secondary employment or conflict of interest declarations
- Information about your use of our technology systems

We use this information to:

- Carry out the contract we have with you
- Comply with and demonstrate compliance with our legal obligations as an employer and any other applicable laws or best practice such as 'Safer Recruitment' practices
- Carry out checks with the Disclosure and Barring Service if you are working with vulnerable adults and children
- Provide you access to business services required for your role and manage our operational and HR processes
- Monitor the security of and prevent unauthorised access to our technology systems

Information related to your finances, salary, pension and loans

We process the following types of personal information:

- Information about your job role and your employment contract including; your start and leave dates, salary (including grade and salary band), any changes to your employment contract, working pattern (including any requests for flexible working)
- Details of payments made to you
- Details of any student loans you have
- Details of any leave including sick leave, holidays, special leave etc.
- Pension details including membership of occupational pension schemes (current and previous)
- Your bank account details, payroll records and tax status information, P45 and P46 documents
- Details relating to Maternity, Paternity, Special, Shared Parental and Adoption leave and pay. This includes forms applying for the relevant leave, copies of MATB1 forms/matching certificates and any other relevant documentation relating to the nature of the leave you will be taking

We process this information to:

- Process the payment of your salary, pension and other employment related benefits
- Carry out the administration of your statutory and contractual leave entitlements such as sick leave, holiday or parental, adoption, paternity or maternity leave
- Prevent fraud

Information relating to your performance and training

We process the following types of personal information:

- Information relating to your attendance and performance at work e.g. probation reviews, development plans, promotions
- Grievance and dignity at work matters and investigations to which you may be a party or witness
- Disciplinary records and documentation related to any investigations, hearings and warnings/penalties issued
- Whistleblowing concerns raised by you, or to which you may be a party or witness (see Whistleblowing Policy)
- Information related to your training history and development needs

We process this information to:

- Assess your performance, to conduct pay and grading reviews
- Deal with any employer/employee related disputes
- Meet the training and development needs required for your role

Under data protection law we need to have a valid legal basis for using your personal information. Depending on the processing activity, we rely on the following lawful basis for processing your personal data under the Data Protection Act 2018:

- Where we need the data to perform the contract we have entered into with you
- Where we need to comply with a legal obligation as your employer
- Because we have decided the processing is necessary for our legitimate interests

Information relating to your health and wellbeing and other special category data

We process some types of sensitive personal data which are subject to additional protection under data protection law. Because of the sensitive nature of this data, we have carried out an assessment to check the processing of this data is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose. We use the special category personal information we hold about you for a number of different purposes, which we list below.

We process the following types of special categories of personal information:

- Details of any access or other needs required for us to make reasonable adjustment to your working conditions
- Health and wellbeing information either declared by you or obtained from health checks, eye examinations, occupational health referrals and reports, sick leave forms or fit notes i.e. Statement of Fitness for Work from your GP or hospital
- Details about your racial or ethnic origin, religious beliefs, disability status and gender identification
- Records of conversations with you about your beliefs where we see it as our duty for the prevention of radicalisation or other aspects of the government's Prevent strategy
- Information about an accidents or incidents that have taken place relating to the workplace

We process this information to:

- Comply with and demonstrate compliance with employment law and best practice and any other applicable laws
- Maintain records of statutory sick pay and maternity pay
- Ensure access or other needs are catered for at interview or selection testing during our recruitment process
- Ensure your health, safety and welfare at work and make any reasonable adjustments needed to help you carry out your role
- Meet our legal requirements to record if you have had an accident or injury at work
- Where we are under duty to report under the Counter-Terrorism and Security Act 2015 to prevent people from being drawn into terrorism and refer any concerns of extremism to the police
- Monitor the diversity of our workforce and comply with our statutory obligations under the Equality Act 2010

Data protection law prohibits us from processing any special category personal information unless we can satisfy at least one of the conditions laid down by data protection law. We must also set out below the

specific conditions we rely upon when processing special category data from Schedule 1 of the Data Protection Act 2018. These are:

- With your explicit consent
- For the purpose of carrying out our obligations and exercising specific rights in the field of employment and social security and social protection law
- For reasons of substantial public interest where processing is necessary for the purposes of preventive or occupational medicine or for the assessment of the working capacity of the employee
- For reasons of substantial public interest for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between groups of people specified in relation to that category with a view to enabling such equality to be promoted or maintained
- To protect your vital interests or those of another person where you are incapable of giving your consent, for example in a medical emergency

In rare cases, where a claim has been brought against Manchester Settlement or there is a potential risk of a legal dispute or claim, we may need to process your special category personal information where it is necessary for the establishment, exercise or defence of legal claims.

We may also process your special category personal data for reasons of substantial public interest where the processing is necessary for the purposes of complying with or assisting other persons to comply with, a regulatory requirement which involves a person taking steps to establish whether another person has committed an unlawful act or been involved in dishonesty, malpractice or other seriously improper conduct.

Because we process certain types of special category personal data, the law says that we must also keep an Appropriate Policy Document that provides more information about this and how we comply with the law.

Personal data about criminal offences

We will only collect information about criminal offences where we are legally able to do so. Criminal offences data includes any information relating to criminal convictions and offences or related security measures. This covers information about offenders or suspected offenders in the context of criminal activity, allegations, investigations and proceedings.

As part of our pre-employment checks or at any time during your employment with us, we will ask you to declare any criminal offences to help us assess the suitability of applicants, volunteers and employees for positions of trust.

As an organisation using the Disclosure and Barring Service (DBS) checking service to help assess the suitability of applicants for positions of trust, we comply fully with the code of practice regarding the correct handling, use, storage, retention and disposal of certificates and certificate information. This code of practice is detailed in our Safer Recruitment for Staff policy and complies fully with its obligations under data protection law and other relevant legislation pertaining to the safe handling, use, storage, retention and disposal of certificate information.

We process criminal offences data because it is necessary for us to comply with the law as set out in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975. In addition to having a lawful basis, we use the special categories condition that processing is necessary for the purposes of performing or exercising obligations or rights which are imposed or conferred by law on the controller or the data subject in connection with employment, social security or social protection.

For more information see our Safe Recruitment for Staff policy.

How we collect and store personal information

We get information about you from the following sources:

- Directly from you
- From UK Visas and Immigration office
- From an employment agency
- From an education establishment if you are a student
- From referees, either external or internal
- From Occupational Health and other health service providers
- From Pension administrators and other government departments, for example from HMRC or the Disclosure Barring Service

Your information is securely stored. We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach set out in our Data Breach Policy.

Electronic records are held for each member of staff or volunteer. Data is held securely on our file storage system, in our electronic online form product Aida Forms and in our Breathe HR system.

Information relating to the recruitment process will be deleted 6 months after the process is completed. Information related to your employment will be retained for 6 years after your employment with us ends.

In relation to data relating to criminal convictions and offences, once a recruitment (or other relevant) decision has been made, we do not keep this information for any longer than is necessary. This retention will allow for the consideration and resolution of any disputes or complaints, or be for the purpose of completing safeguarding audits.

Who we share your information with

From time to time we will need to share your information with external people and organisations. We will only do so where we have a legitimate or legal basis for doing so and in compliance with our obligations under data protection law.

This may include government agencies and external auditors. For example, we may share information about you with HMRC for the purpose of collecting tax, processing student loan deductions and national insurance contributions.

We will also share data with OFSTED for the purpose of maintaining a Single Central Record as part of our Safer Recruitment obligations. We may share your information with the police, the courts and any other government department, such as the Home Office and the Disclosure Barring Service (but only if us doing so is lawful).

We may share data with our insurance companies or professional advisors when they need it to give us their professional advice. This includes sharing your data with occupational health and other medical professionals including social and welfare organisations to provide us with medical opinions

in relation to any medical condition, illness or disability you may have or develop during the course of your employment/engagement.

There may be circumstances where we are permitted to process and share your special category personal data relating to health where it is essential for someone's life and you are not capable of giving your consent, for example in relation to a medical emergency.

We will also share some of your financial details with third parties such as our accountant and payroll provider for the purpose of managing our finances and your pension contributions.

We may also share your data with providers of goods and services who have contracts with us such as companies that supply technical solutions and business support.

Requests for references

Your information may be disclosed to the referees you have provided on your application form in order to obtain references and/or with education, professional and vocational establishments to verify information you have provided on your application form or during any interview process.

If you leave, or are thinking of leaving, we may be asked by your new or prospective employers to provide a reference. For example, we may be asked to confirm the dates of your employment or your job role. If you are still employed by us at the time the request for a reference is received, we will discuss this with you before providing this.

CCTV

The Manchester Settlement building is monitored using CCTV. CCTV surveillance is intended for the purposes of:

- Promoting the health and safety of children, staff and visitors
- Protecting the building and resources.

Cameras are placed around the building inside and outside, but not in the toilets or changing areas. You can find out more about our use of CCTV and your rights under data protection law in our CCTV Policy.

Automated decision making or monitoring

We do not carry out any automated decision-making or profiling in relation to you. This includes automated processing of personal data to evaluate personal aspects, in particular to analyse or predict aspects concerning suitability for a role, performance at work, economic situation, health, personal preferences, behaviour or location/movements.

Your rights in relation to this processing

Under certain circumstances, by law you have the right to:

- **Request access to your personal information** (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. You can request your personnel data by emailing a Subject Access Request to admin@manchestersettlement.org.uk. This includes footage of images of you from CCTV.
- **Request correction of the personal information** that we hold about You. This enables you to have any incomplete or inaccurate information we hold about You corrected.
- **Request erasure of your personal information.** This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it.

You also have the right to ask us to delete or remove Your personal information where You have exercised Your right to object to processing (see below).

- **Object to processing of your personal information** where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground.
- **Request the restriction of processing of your personal information.** This enables you, as is appropriate, to ask us to suspend the processing of personal information about you for example if You want us to establish its accuracy or the reason for processing it.
- **Request the transfer of your personal information to another party.**

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact our Data Protection Officer in writing.

No fee usually required: You will not have to pay a fee to access your personal information (or to exercise any of the other rights). If you make a request, we have one month to respond to you. We will always seek to comply with your request however we may be required to hold or use your information to comply with legal duties.

Changes to this privacy notice

We reserve the right to update this privacy notice at any time, and we will provide or publish a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

Where to go if you want more information about your rights or to make a complaint

For more information or any questions about your data or this privacy notice, please contact our Data Protection Officer through admin@manchestersettlement.org.uk or 01619741300

The Information Commissioner's Office (ICO) regulates data protection and privacy matters in the UK. They make a lot of information accessible on their website and they ensure that the registered details of all data controllers such as ourselves are available publicly. You can access them [here](#).

You can make a complaint to the ICO at any time about the way we use your information. However, we hope that you would consider raising any issue or complaint you have with us first. We will always do our very best to solve any problems you may have.

To contact the ICO, telephone their helpline on 0303 123 1113 or go to their [website](#).

Other relevant policies:

- Data Protection Policy
- Data Breach Policy
- Subject Access Request Policy
- CCTV Policy
- Record of Personal Data and Processing
- Safe Recruitment of Staff Policy
- Whistleblowing Policy
- Appropriate Policy Document