Manchester Settlement
widening horizons since 1895

Data Protection Policy

Policy Status:	Statutory
Review Cycle:	2
Policy Reference:	

Review Date	Author	Changes
01/02/16	AB	Compliance Review
01/11/18	AB and advisor	Updated as part of the introduction of all GDPR compliant processes

1. Contents

1. Introduction 2
2. Notification of Data Held and Processed 2
3. The Data Controller and the Designated Data Controllers 2
4. Information Held 3
5. Processing of Personal Information 3
6. Telephone conversations and Meetings 4
7. Sensitive Personal Data 4
8. Personnel files 4
9. Portable Devices 5
10. Working from Home or Other Off Site Premises 5
11. Data subject access requests 5
12. Correction, updating and deletion of data 6
13. Data that is likely to cause substantial damage or distress 6
14. Employees' obligations regarding personal information 6
15. Consequences of non-compliance 7
16. Review of procedures and training 7

2. Introduction

Manchester Settlement needs to keep certain information about its employees, trustees, volunteers, members, clients and other members of the public to enable it to monitor performance and achievements. It is also necessary to process information so that staff can be recruited and paid, activities organised and legal obligations to funding bodies and government fulfilled.

To comply with the law, information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. To do this, Manchester Settlement must comply with the Data protection Act 1998 (the Act). In summary these state that personal data must be:

i) obtained and processed fairly and lawfully;
ii) obtained for a specific and lawful purpose and not processed in any manner incompatible with that purpose;
iii) adequate, relevant and not excessive for that purpose;
iv) accurate and kept up to date
v) not to be kept longer than necessary;
vi) processed in accordance with the data subject's rights;
vii) kept safe unauthorised access, accidental loss or destruction;
viii)not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

All Manchester Settlement staff and volunteers who process or use information must ensure that they follow these principles at all times. In order to ensure that this happens, Manchester Settlement has adopted this Data Protection Policy.

Any member of staff, trustee or volunteer, who considers that this policy has not been followed in respect of personal data about him/herself, should be raised as a formal grievance.

3. Notification of Data Held and Processed

All employees, trustees, volunteers, members, clients and other members of the public have the right to:

know what information Manchester Settlement holds and processes about them and why
know how to gain access to it;
know how to keep it up to date;
know what Manchester Settlement is doing to comply with its obligations under the Act.

4. The Data Controller and the Designated Data Controllers

Manchester Settlement as a charity is the Data Contoller under the Act, and the organisation is therefore ultimately responsible for the implementation. However, Designated Data Controllers will deal with day to day matters.

Manchester Settlement has one Designated Controller, the current responsibility holder name is available from the main office.

5. Information Held

Personal Information is defined as any details relating to a living identifiable individual. Within Manchester Settlement this applies to employees, trustees, volunteers, members, clients and other members of the public such as job applicants and visitors. We need to ensure that information relating to all these people is treated correctly and with appropriate degree of confidentiality.

Manchester Settlement holds Personal Information in respect of its employees, trustees, volunteers, members, clients and other members of the public. The information held may include an individual's name, postal, e-mail and other addresses, telephone and facsimile numbers, subscription details, organisational roles and membership status.

Personal Information is kept in order to enable the Manchester Settlement to understand the history and activities of individuals or organisations within the voluntary and community sector and to effectively deliver services to its members and clients.

All sensitive personal data will be processed in accordance with the eight data protection principles.

Some Personal Information is defined as Sensitive Data and needs to be handled with special care (see paragraph 7 below).

6. Processing of Personal Information

All staff and volunteers who process or use any Personal Information are responsible for ensuring that:

Any Personal Information which they hold is kept securely; and
Personal Information is not disclosed either orally or in writing or otherwise to any unauthorised third party.

Staff and volunteers should note that unauthorised disclosure will usually be a disciplinary matter, and may be considered gross misconduct in some cases.

Personal information should be:
kept in a locked filing cabinet; or
in a locked drawer; or

- in a locked room; or
- if it is computerised, be password protected; or
- kept only on disk which is itself kept securely.

7. Telephone conversations and Meetings

If personal information is collected by telephone, callers should be advised what that information will be used for and what their rights are according to the Act.
Personal or confidential information should preferably not be discussed in public areas of Manchester Settlement work premises or within open –plan office areas.

8. Sensitive Personal Data

"Sensitive personal data" is information about an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or other beliefs of a similar nature;
- trade union membership (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);
- physical or mental health or condition;
- sex life;
- commission or alleged commission of any criminal offence; and
- proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

The organisation will not retain sensitive personal data without the express consent of the employee in question.

The organisation will process sensitive personal data, including sickness and injury records and references, in accordance with the eight data protection principles. If the organisation enters into discussions about a merger or acquisition with a third party, the organisation will seek to protect employees' data in accordance with the data protection principles.

9. Personnel files

An employee's personnel file is likely to contain information about his/her work history with the organisation and may, for example, include information about any disciplinary or grievance procedures, warnings, absence records, appraisal or performance information and personal information about the employee including address details and national insurance number.

There may also be other information about the employee located within the organisation, for example in his/her line manager's inbox or desktop; with payroll; or within documents stored in a relevant filing system.

The organisation may collect relevant sensitive personal information from employees for equal opportunities monitoring purposes. Where such information is collected, the organisation will anonymise it unless the purpose to which the information is put requires the full use of the individual's personal information. If the information is to be used, the organisation will inform

employees on any monitoring questionnaire of the use to which the data will be put, the individuals or posts within the organisation who will have access to that information and the security measures that the organisation will put in place to ensure that there is no unauthorised access to it.

The organisation will ensure that personal information about an employee, including information in personnel files, is securely retained. The organisation will keep hard copies of information in a locked filing cabinet. Information stored electronically will be subject to access controls and passwords and encryption software will be used where necessary.

10. Portable Devices

Where laptops or other portable computing devices are taken off site, employees must follow the organisation's relevant policies relating to the security of information and the use of computers for working at home/bringing your own device to work.

11. Working from Home or Other Off Site Premises

Employees are responsible for the security of data as per this policy when working from other sites.

12. Data subject access requests

The organisation will inform each employee of:

- the types of information that it keeps about him/her;
- the purpose for which it is used; and
- the types of organisation that it may be passed to, unless this is self evident (for example, it may be self evident that an employee's national insurance number is given to HM Revenue & Customs).

An employee has the right to access information kept about him/her by the organisation, including personnel files, sickness records, disciplinary or training records, appraisal or performance review notes, emails in which the employee is the focus of the email and documents that are about the employee.

The organisation will charge £10 for allowing employees access to information about them. The organisation will respond to any data subject access request within 40 calendar days.

The organisation will allow the employee access to hard copies of any personal information. However, if this involves a disproportionate effort on the part of the organisation, the employee shall be invited to view the information on-screen or inspect the original documentation at a place and time to be agreed by the organisation.

The organisation may reserve its right to withhold the employee's right to access data where any statutory exemptions apply.

13. Correction, updating and deletion of data

The organisation has a system in place that enables employees to check their personal information on a regular basis so that they can correct, delete or update any data. If an employee becomes aware that the organisation holds any inaccurate, irrelevant or out-of-date information about him/her, he/she must notify the organisation immediately and provide any necessary corrections and/or updates to the information.

14. Data that is likely to cause substantial damage or distress

If an employee believes that the processing of personal information about him/her is causing, or is likely to cause, substantial and unwarranted damage or distress to him/her or another person, he/she may notify the organisation in writing to request the organisation to put a stop to the processing of that information.

Within 21 days of receiving the employee's notice, the organisation will reply to the employee stating either:

- that it has complied with or intends to comply with the request; or
- the reasons why it regards the employee's notice as unjustified to any extent and the extent, if any, to which it has already complied or intends to comply with the notice.

15. Employees' obligations regarding personal information

If an employee acquires any personal information in the course of his/her duties, he/she must ensure that:

- the information is accurate and up to date, insofar as it is practicable to do so;
- the use of the information is necessary for a relevant purpose and that it is not kept longer than necessary; and
- the information is secure.
- In particular, an employee should ensure that he/she:
- uses password-protected and encrypted software for the transmission and receipt of sensitive emails;
- sends fax transmissions to a direct fax where possible and with a secure cover sheet; and
- locks files in a secure cabinet.

Where information is disposed of, employees should ensure that it is destroyed. This may involve the permanent removal of the information from the server, so that it does not remain in an employee's inbox or trash folder. Hard copies of information may need to be confidentially shredded. Employees should be careful to ensure that information is not disposed of in a wastepaper basket/recycle bin.

If an employee acquires any personal information in error by whatever means, he/she shall inform Designated Data Controller immediately and, if it is not necessary for him/her to retain that information, arrange for it to be handled by the appropriate individual within the organisation.

An employee must not take any personal information away from the organisation's premises [save in circumstances where he/she has obtained the prior consent to do so].

If an employee is in any doubt about what he/she may or may not do with personal information, he/she should seek advice from Designated Data Controller. If he/she cannot get in touch with them, he/she should not disclose the information concerned.

16. Consequences of non-compliance

All employees are under an obligation to ensure that they have regard to the eight data protection principles when accessing, using or disposing of personal information. Failure to observe the data protection principles within this policy may result in an employee incurring personal criminal liability. It may also result in disciplinary action up to and including dismissal. For example, if an employee accesses another employee's employment records without the requisite authority, the organisation will treat this as gross misconduct and instigate its disciplinary procedures. Such gross misconduct will also constitute a criminal offence.

17. Review of procedures and training

The organisation will provide training to all employees on data protection matters on induction and on a regular basis thereafter. If an employee considers that he/she would benefit from refresher training, he/she should contact Designated Data Controller.

The organisation will review and ensure compliance with this policy at regular intervals.

18. Privacy Notices

This general policy is supported by Privacy Notices that issued to different stakeholders relevant to different areas of our operation. These notices may additionally be supported by easy to understand guides

- For Employees/Volunteers
- For Childcare Parents/Carers
- For Housing Service users
- For Community Service users

19. Related Policies/Procedures

Staff Use of ICT Statement
Subject Access request Procedure
Data Breach Policy
Data Retention Policy