



# Data Protection Policy

## Contents

- A. General principles
- B. Personal information relating to staff
  - 1. General
  - 2. What information we hold
  - 3. Why we hold information
  - 4. Where we hold the information
  - 5. How we use the information
  - 6. How long we keep the information
  - 7. Information technology
  - 8. Monitoring of staff activity
  - 9. References
  - 10. Subject access requests
  - 11. Obligations of staff
  - 12. Guidelines on disclosing information to internal and external sources
  - 13. Organisational information
- C. Personal information relating to service users
  - 1. General
  - 2. What information we hold
  - 3. Why we hold the information
  - 4. Where we hold the information
  - 5. Collecting, recording and accessing data
  - 6. Passing on information
  - 7. Collecting and safeguarding information
  - 8. Subject access requests
- D. Personal information relating to volunteers
  - 1. General
  - 2. What information we hold
  - 3. Why we hold information
  - 4. How we collect and hold information
  - 5. How we use the information
  - 6. How long we keep the information

7. Information technology
  8. Monitoring of online activity
  9. References
  10. Subject access requests
  11. Obligations of volunteers
  12. Guidelines on disclosing information to internal and external sources
  13. Organisational information
- E. Exceptions: breaking confidentiality

## APPENDICES

- Privacy notice for staff
- Staff confidentiality statement
- Privacy notice for clients
- Client consent form
- Privacy notice for volunteers
- Volunteer confidentiality statement

## A. General Principles

- A1. Manningham Project Ltd recognises the right to privacy of the individual as a basic human right. We accept that personal details about an individual belong to that individual. Accordingly we undertake to respect the confidentiality of certain information.
- A2. Personal data is defined as “information about a living individual who is identifiable by that information, or who could be identified by the information combined with other data”. It includes names, addresses, identifying descriptions and information relating to individuals such as bank details or personal attributes.
- A3. Confidential information is defined as verbal or written information which is not meant for public or general knowledge, or information which is regarded as personal by clients, members, trustees, staff or volunteers. It includes expressed opinion about a person or intentions regarding a person.
- A4. This policy relates to the protection of the privacy of staff, volunteers, job applicants, trustees, Manningham Project Ltd members, service users and any other person about whom Manningham Project Ltd holds personal information of a formal or an informal nature.
- A5. Confidentiality is based upon a reasoned concern for the interests of the person to whose personal information Manningham Project Ltd has access. Respecting confidentiality means that information may be disclosed only with consent or when necessary in law, and that consultation and discussion remains within those boundaries. This protects the integrity of both Manningham Project Ltd and of individuals.
- A6. Where there is uncertainty about issues around confidentiality, advice should be sought from line managers and, where appropriate, trade unions.
- A7. **Failure to observe this policy or misuse of personal data is a disciplinary offence and may even constitute a criminal offence.** Please refer especially to the section titled “Staff obligations”.

- A8. **Data Protection Act 2018.** Manningham Project Ltd takes seriously its obligations under the Data Protection Act 2018 and the General Data Protection Regulation (GDPR). We are registered with the Information Commissioner. Our registration, which is renewed annually, allows us to collect, store and use certain personal information following strict guidelines. These guidelines define the purposes for which we hold information: in our case, this is information for the purposes of recording our work with clients, staff administration, fundraising and realising our charitable objectives.
- A9. Within these groups, the guidelines define the data subjects (i.e. the individuals about whom that information is held), the classes of data (i.e. what kind of information is held) and the data recipients (i.e. who has access to it).
- A10. The Data Protection Act sets out the following six data protection principles which must be adhered to with respect to personal data:
- Data processing must be lawful and fair;
  - The purposes of data processing must be specified, explicit and legitimate;
  - Personal data must be adequate, relevant and not excessive;
  - Personal data must be accurate and kept up to date;
  - Personal data must be kept for no longer than is necessary;
  - Personal data must be processed in a secure manner.

Manningham Project Ltd will comply with these requirements and will extend the principles of data protection to apply to all forms of personal information.

## **B. Personal Information Relating to Staff**

### **B1. General**

B1.1 Manningham Project Ltd holds information about employees to do with their working life in order to fulfil its responsibilities as an employer. Much of this information is highly personal and Manningham Project Ltd recognises its duty to safeguard the data by all means possible and to notify staff about what is kept and why, along with information about how the data can be accessed and by whom.

### **B2. What information we hold**

B2.1 Information held by Manningham Project Ltd will include:

- Information relating to recruitment and selection such as application forms; references; shortlisting and interview assessments; proof of eligibility to work in the UK; where relevant, unspent criminal records and/or the outcome of DBS investigations;
- Personal details of home address, phone number, next of kin;
- Information necessary for payment of salaries, such as bank details, national insurance number, details of deductions, expenses claims;
- Information about academic and vocational qualifications and experience;
- Notes of probationary and annual reviews and supervisions;
- Sick notes, and medical assessments, including information relating to disabilities;
- Absence records, including sickness absence, compassionate leave, unauthorised absences;

- Time sheets and holiday sheets;
- Details of grievance and disciplinary proceedings including current warnings (within the timescales allowed by the appropriate policies);
- Reference requests and responses.

B2.2 More sensitive information might include information about your health and any medical condition or disability. We would only use this to ensure your health and safety in the workplace.

### **B3. Why we hold information**

B3.1 The data kept on staff is primarily in relation to their employment with Manningham Project Ltd. This data will be used as necessary for the administering and managing their employment and where needed for compliance with our legal obligations.

B3.2 Information may also be used for other legitimate interests of Manningham Project Ltd, such as for the purposes of applying for funding, obtaining insurance or responding to requests for information from funding bodies, the Charity Commissioners or other reputable bodies.

B3.3 Where possible, sensitive information will not be tied to individuals but will be given in anonymised statistical formats only. No unrelated data will be kept and any sensitive data (excluding health and criminal records) held by the organisation will be deleted at the request of the individual concerned.

### **B4. How we collect and hold information**

B4.1 We collect personal information about staff and prospective employees mainly from the individuals concerned.

B4.2 Sometimes, particularly during recruitment, we may seek information from third parties including employment agencies, former employers, referees, credit reference agencies and or other background check providers. We will normally seek consent to do so.

B4.3 If concerns arise about occupational health then we may seek independent medical evidence, but only with explicit consent of the staff concerned.

B4.4 All personnel data is kept either in locked filing cabinets and /or in password protected computer files. Most personal data is kept in individual personnel files in the Project Manager's filing cabinet which is kept locked. Other data (e.g. bank details, NI number) is kept by the Project Manager in a locked filing cabinet. The Project Manager keeps staff files covering supervision sessions plus any job-related information necessary for management.

B4.5 Some personal information, including names and photographs, may be published in e.g. newsletters, annual reports, publicity leaflets or the organisation's website, but only after staff have freely given their consent to do so. This information will not include home or personal contact details.

### **B5. How we use information**

B5.1 Access to staff data is restricted to management at the appropriate level or to senior administrative staff on a 'need to know' basis. Information may also be disclosed as required by law, contract or on a 'need to know' basis to trustees,

auditors, pension providers, funders, insurers, government departments or other relevant parties/individuals.

B5.2 Job applicants are also covered by the Data Protection Act and by this policy. Manningham Project Ltd will design and process application forms and other information relating to applicants in line with the Act.

B5.3 Manningham Project Ltd will only request information which is relevant and not excessive and for the particular purposes of the selection process only. This information will be securely stored and will only be accessed by staff that need to have it for purposes of administration or selection. It will not be kept for longer than necessary for the needs of the organisation, normally six months for unsuccessful candidates.

B5.4 Sensitive information relating to health, disability, criminal records and immigration status will only be requested where necessary for the protection of the interests of the data subject, or the organisation and/or its service users and will not be disclosed to anyone who does not need to know. Sensitive information relating to gender, age, ethnicity and disability may be requested but will be used for equality and diversity monitoring purposes only. This information will not form part of the selection process and will not be retained in any form which identifies the individual to whom it pertains.

B5.5 The identity of job applicants will be kept confidential as far as possible and for as long as possible. Where a job offer is made, the names of the successful candidates will not be disclosed until the appointment has been accepted and confirmed.

## **B6. How long we keep information**

B6.1 Most information will be retained for as long as a person is employed by Manningham Project Ltd and for a reasonable period of time thereafter, not exceeding 6 years. Disciplinary proceedings and warnings will be kept for the time stipulated in the policy concerned. Recruitment papers from unsuccessful applicants to a job will be kept for a reasonable period of time not exceeding one year. DBS documentation will not be retained although a record will be kept of the fact that a satisfactory/unsatisfactory DBS check has been made. This will be kept on file for as long as necessary, or until the next DBS check is carried out.

## **B7. Information technology**

B7.1 Personal data held on computers (including files, emails, databases etc) and personal data downloaded from the web are subject to the same control and restrictions as paper-based data. Staff must take particular care when using any personal data in these contexts. In particular, no personal information should be posted on the internet in any circumstances without compelling reasons and the explicit consent of the individual to whom the information relates.

## **B8. Monitoring of staff activity**

D8.1 Staff should be aware that Manningham Project Ltd may, if they have reason to do so, monitor use of the internet and/or emails. Private emails will never be opened intentionally but staff should be aware of the possibility of accidental access and of the right of managers to question and investigate private use.

Deliberate monitoring will only take place where there are reasonable grounds to suspect a disciplinary offence or another justified concern. Please see the ICT Use policy. Performance and quality control monitoring will be overt and for a clear purpose.

## **B9. References**

B9.1 References given by an employer about a person currently working for them are exempt from some aspects of normal data protection rules. This means that an employee has no automatic right of access to a reference written about them by Manningham Project Ltd. However Manningham Project Ltd will normally only respond to reference requests that are authorised by the employee concerned.

B9.2 As a general rule, employment-related references should only be given by the Project Manager. However, management committee members may provide references for staff where appropriate, provided these are checked and authorised prior to sending by the Project Manager. Personal references should be clearly stated as such and should not be on Manningham Project Ltd headed paper. References must be objective, truthful and justifiable. Telephone references should not be given unless you have been asked to provide one by the person whom the reference concerns, and then you should initiate (or return) the phone call to the person to whom the reference is to be given to confirm identity.

B9.3 Referees should bear in mind that although there is no automatic right for the subject of the reference to see it before it is sent, they will usually have a right to access any references written about them once they are received by a new/prospective employer.

## **B10. Subject access requests**

B10.1 Staff are entitled to see their own personnel files. To do so, they should arrange a mutually convenient time with their line manager. Access may be denied or limited where it involves disclosing information about or from an identified third party (e.g. a colleague) unless the third party concerned has given consent to the disclosure of that information.

B10.2 As well as taking action to protect third party confidentiality, Manningham Project Ltd will not respond to subject access requests which:

- disclose any information relating to management forecasts where this could jeopardise the business effectiveness of the organisation;
- or reveal legal proceedings against an individual, except to those directly concerned.

## **B11. Obligations of Staff and Volunteers**

B11.1 The Project Manager is the Registered Data Controller and is responsible for notification to the Information Commissioner. S/he should be deferred to with any questions relating to data protection or confidentiality (see Appendix: *Procedures Relating to Personal Data Breaches*). However, **all staff and volunteers** are responsible for ensuring compliance with this policy. They must:

- Ensure that they have read and understood this policy as it relates to them;

- Ensure that data which they supply or for which they are responsible is up-to-date, accurate, fair and relevant to its purpose, including information about themselves. Staff must notify the organisation of any changes in circumstance to enable the organisation to update personnel records accordingly;
- Not keep any records on other individuals (whether clients/employees of Manningham Project Ltd or members or service users of other organisations) which are unnecessary, incorrect or which contain unfounded opinion or speculation;
- Not share personal information about other members of staff or partner agency staff/their clients or other service users (e.g. sickness, personal circumstances), that they know as a result of handling confidential information (e.g. quality of advice assessments, sick notes, application forms) or which is disclosed in confidential settings (e.g. supervision or other one to one meetings), without that person's unambiguous agreement;
- Keep data secure. Paper and external computer files must be locked up, computers must be password protected; laptops and computer disks containing personal information, open computer screens, or open paper files must not be left unattended;
- Not disclose, share or transfer outside the organisation any personal information relating to other staff, volunteers, trustees, or partner agency staff/their clients or other service users without the explicit consent of the individual concerned;
- Dispose of personal data safely. Paper notes and records must be shredded or disposed of as 'confidential waste'. Hard drives of redundant PCs must be wiped clean before disposal.

B11.2 Particular care must be taken where personal data is processed 'off-site', at home or in other locations. This presents a greater risk of loss, damage or theft and staff must take appropriate security precautions.

B11.3 Staff will be provided with a copy of the Manningham Project Privacy Notice for Staff and will be required to read the Data Protection Policy and to sign the Staff Confidentiality Statement.

B11.4 Volunteers will be provided with a copy of the Manningham Project Privacy Notice for Volunteers and will be required to read the Data Protection Policy and to sign the Volunteers Confidentiality Statement.

B11.5 Any incident or circumstance resulting in either significant risk of a breach of security of any personal data or in an actual breach must be reported to the Project Manager and recorded in the Project's incident book. See Appendix: *Procedures Relating to Personal Data Breaches*

## **B12. Guidelines on disclosing information to internal and external sources**

B12.1 Internal information sharing: Manningham Project Ltd recognises that trustees, staff, volunteers and members may need to share personal information with others internally within Manningham Project Ltd. This might include, for instance, discussion of issues in partner agencies during supervision, discussion of situations to gain experience and opinion from

colleagues, “on the job” training. Care must be taken that this kind of information sharing is not done publicly or where it can be overheard. Such conversations should, where appropriate, be held without explicitly identifying the individual or organisation under discussion.

## **B12.2 Supervision**

B12.2.1 Supervision sessions are in general confidential to the supervisor, the Project Manager and the Trustees of the organisation.

B12.2.2 Ground rules for when and why confidentiality may be broken should be agreed at the start of a supervision relationship and might include, for instance:

- information about the progress of work against funding targets;
- complex or problematic case management;
- discussion of the implications for colleagues of a request for flexible working;
- some information to colleagues about personal circumstances which are temporarily affecting performance;
- discussion of grievances or concerns about performance with a more senior manager.

B12.2.3 Wherever possible, agreement about any breach of confidentiality should be reached in advance of the disclosure taking place. Although the supervisor is bound by confidentiality, it is helpful for the supervisee to inform the supervisor if there are any personal circumstances which are particularly sensitive.

## **B12.3 Answering requests for personal staff information**

B12.3.1 Personal information about a colleague should not usually be discussed with other staff or people outside Manningham Project Ltd without that person’s permission. Personal details including address and phone number, health matters or personal circumstances may not be passed on without explicit consent.

B12.3.2 It is usually safe to reveal a colleague’s work contact (telephone and email address) in response to an enquiry regarding a work function. However, staff must not reveal personal details of other staff members to unknown or unverified external sources, even where these claim to be family members, friends, Government bodies or the police. Strategies to deal with such enquiries could include:

- Asking the enquirer to put their query in writing or into an email, if appropriate backed up by documentary evidence to support the request.
- Informing the enquirer that a message will be passed on, either asking the person to contact the enquirer directly or agreeing to pass on a sealed envelope/incoming email message to the person;
- Telling the enquirer that you will phone back once you have collected/verified the information required.

## **B13. Organisational information**

B13.1 Trustees, staff, volunteers and members are bound by confidentiality in all matters relating to the internal affairs of Manningham Project Ltd. Confidential information concerning Trustee Board meetings, staff meetings, finances, recruitment, planning, etc should not be disclosed outside the organisation unless authorisation is given to do so. This does not apply to disclosures



made under the Public Interest Disclosure Act (“whistle blowing”). See also Subject Access Requests above.

B13.2 No statements concerning internal matters or policy may be made to the media without the express permission of the Project Manager

## **C. Personal Information relating to service users and to partner agencies, their clients and their staff**

### **C1. General**

C1.1 Manningham Project Ltd is committed to respecting the confidentiality of their clients/staff and others who use or support Manningham Project Ltd services. This means respecting the right of Manningham Project Ltd members, their staff and clients, benefactors, beneficiaries and other service users to privacy and their right to expect that any personal information they give us will not be discussed or passed on to anyone without their permission.

C1.2 Please refer to “staff obligations” above for general instructions on the collection, use, storage and disposal of all personal information associated with the Manningham Project Ltd

### **C2. What information we hold**

C2.1 Personal or sensitive information about Manningham Project Ltd’s clients/staff and other service users could include names and addresses, personal circumstances, membership details, financial and organisational arrangements, case records/client advice issues and internal organisational issues/disputes. The information may be given in conversation or in written form, for example on an application/interview form, as part of a meeting or assessment process or by email.

### **C3. Why we hold this information**

C3.1 Manningham Project Ltd keeps information on Manningham Project Ltd’s clients/staff and other service users for the purposes of providing its services. It keeps information for applying for funding, monitoring how funds are spent, responding to request for information from Government offices, the Charity Commission and other reputable organisations.

C3.2 Statistical and depersonalised information may be used for campaigning or publicity purposes. No unrelated data will be kept and any sensitive data held by the organisation will be deleted at the request of the individual concerned.

C3.3 The sole legal basis for Manningham Project Ltd. to hold and process client information is the client’s explicit, informed consent. See Section D for exceptional situations in which this may be over-ridden by other legal requirements.

### **C4. Where we hold the information**

C4.1 All personal data is kept in locked filing cabinets and/or in password protected computer files.

### **C5. Collecting, recording and accessing data**

- C5.1 All information we hold concerning clients is provided by clients themselves, or from other sources if clients give explicit consent.
- C5.2 Clients will be provided with a copy of the Manningham Project Ltd. Privacy Notice for Clients and required to complete and sign the 'Client's Consent to Use Personal Information'.
- C5.3 Written records of any dealings with clients/service users of the Manningham Project Ltd or its member organisations may be made with the client's permission if the purpose of such records is clearly explained to the client. Only essential information should be recorded and these records must be processed in line with Data Protection principles, stored securely and destroyed when no longer needed.

## **C6. Passing on information**

- C6.1 Where information about a Manningham Project Ltd's or its clients/staff is to be shared with a **partner organisation**, the relevant person must confirm their agreement by giving signed authorisation, normally in the relevant section of the Client Consent form.
- C6.2 Where funders require personal information about the beneficiaries of services for audit purposes, this information will be collected on forms which clearly indicate who will receive the information and include provision for service users to sign a consent declaration.
- C6.3 Personal information should not be conveyed to other organisations or individuals via telephone calls, faxes or emails without adequate safeguards regarding confidentiality.
- C6.4 External requests for information about an individual should not be agreed to. Where appropriate, staff may agree to pass on the request to that individual to respond to if they so choose. See advice above for strategies for dealing with requests for information from unknown or unverified enquirers.
- C6.5 Email communications may not be private – please see ICT Use policy.
- C6.6 Names or contact details should never be released to the media in response to requests for "case studies.
- C6.7 Statistical information may be used for research, monitoring and funding purposes but must not be attributable to an individual. Where, for publicity purposes, Manningham Project Ltd wishes to use an attributed quotation from a client or service user the individual's express permission must be sought before this can be used.

## **C7. Collecting and safeguarding information**

- C7.1 Manningham Project Ltd also recognises its duty to safeguard the information it holds on external groups and individuals. Manningham Project Ltd will regularly update information, dispose of outdated data and check that storage and archive systems are secure.
- C7.2 All **written materials** will be designed to ensure that only necessary data is being collected and that this is kept with permission.

## **C8. Subject access requests**

C3.1 Any member of staff/trustee board or service user of Manningham Project Ltd, is entitled to know what information is held about them, why and where it is held and who can access it. They have the right to see this information and to correct it if necessary. In order to see information, they should contact the Project Manager who will arrange a mutually convenient time for this or who will facilitate the involvement of other relevant staff.

## **D. Personal Information Relating to Volunteers (including Trustees)**

### **D1. General**

D1.1 Manningham Project Ltd holds information about volunteers only for the purposes of recruitment and selection and for managing their activities while working with us as a volunteer. Manningham Project Ltd recognises its duty to safeguard volunteers' data to notify them about what is kept and why, along with information about how the data can be accessed and by whom.

### **D2. What information we hold**

D2.1 Information held by Manningham Project Ltd will include:

- Personal contact details including name, title, addresses, telephone numbers and personal email addresses, date of birth, gender.
- Recruitment information including references and information included in a CV or cover letter as part of the application process. Other relevant information might include: qualifications obtained, language skills, copy of Disclosure and Barring Service Certificate where needed, information about criminal convictions and offences where the law allows.
- More sensitive information might include information about health and any medical condition or disability. We would only use this to ensure a volunteer's health and safety in the workplace.
- We will also maintain records of your volunteer activities undertaken at the Manningham Project and of related supervision meetings.

### **D3. Why we hold information**

D3.1 The data kept on volunteers solely in relation to their work with Manningham Project Ltd. and will be used as necessary for the administering and managing their activities and where needed for compliance with any legal obligations.

D3.2 Anonymised information about volunteering may also be used for other legitimate interests of Manningham Project Ltd, such as for the purposes of applying for funding, obtaining insurance or responding to requests for information from funding bodies, the Charity Commissioners or other reputable bodies.

D3.3 Any legitimate requests for sensitive information concerning volunteers will not be tied to individuals but will be given in anonymised statistical formats only. No unrelated data will be kept and any sensitive data (excluding health and criminal records) held by the organisation will be deleted at the request of the individual concerned.

#### **D4. How we collect and hold information**

D4.1 We collect personal information about volunteers and prospective volunteers mainly from the individuals concerned.

D4.2 During recruitment, we may seek information from referees and will normally seek consent to do so.

D4.3 Applicants will be provided with a copy of the Manningham Project Ltd. Privacy Notice for Volunteers and required to complete and sign the 'Volunteer's Consent to Use Personal Information'.

D4.4 All personal data is kept either in locked filing cabinets and /or in password protected computer files. Most personal data is kept in individual files in the Project Manager's filing cabinet which is kept locked.

D4.5 Some personal information, including names and photographs, may be published in e.g. newsletters, annual reports, publicity leaflets or the organisation's website, but only after individuals have freely given their consent to do so. This information will not include home or personal contact details.

#### **D5. How we use information**

D5.1 Access to volunteer data is restricted to management at the appropriate level or to senior administrative staff on a 'need to know' basis.

D5.2 Volunteering applicants are also covered by the Data Protection Act and by this policy. Manningham Project Ltd will design and process application forms and other information relating to applicants in line with the Act.

D5.3 Manningham Project Ltd will only request information which is relevant and not excessive and for the particular purposes of the selection process only. This information will be securely stored and will only be accessed by staff that need to have it for purposes of administration or selection. It will not be kept for longer than necessary for the needs of the organisation, no more than one month for unsuccessful applicants.

D5.4 Sensitive information relating to health, disability, criminal records and immigration status will only be requested where necessary for the protection of the interests of the data subject, or the organisation and/or its service users and will not be disclosed to anyone who does not need to know. Sensitive information relating to gender, age, ethnicity and disability may be requested but will be used for equality and diversity monitoring purposes only. This information will not form part of the selection process and will not be retained in any form which identifies the individual to whom it pertains.

#### **D6. How long we keep information**

D6.1 Most information will be retained for as long as a person is a volunteer with Manningham Project Ltd and for a reasonable period of time thereafter, not exceeding 6 years. DBS documentation will not be retained although a record will be kept of the fact that a satisfactory/unsatisfactory DBS check has been made. This will be kept on file for as long as necessary, or until the next DBS check is carried out.

#### **D7. Information technology**

D7.1 Personal data held on computers (including files, emails, databases etc) and personal data downloaded from the web are subject to the same control and restrictions as paper-based data. You must take particular care when using any personal data in these contexts. In particular, no personal information should be posted on the internet in any circumstances without compelling reasons and the explicit consent of the individual to whom the information relates.

#### **D8. Monitoring of online activity**

D8.1 You should be aware that Manningham Project Ltd may, if they have reason to do so, monitor use of the internet and/or emails. Private emails will never be opened intentionally but you should be aware of the possibility of accidental access and of the right of managers to question and investigate private use. Deliberate monitoring will only take place where there are reasonable grounds to suspect a disciplinary offence or another justified concern. Please see the ICT Use policy.

#### **D9. References**

D9.1 References given by an employer about a person currently working or volunteering for them are exempt from some aspects of normal data protection rules, which means that you do not have an automatic to see a reference written about you before it is sent. However Manningham Project Ltd will normally only respond to reference requests that you have authorised us to provide.

D9.2 As a general rule, employment-related references should only be given by the Project Manager. However, management committee members may provide references where appropriate, provided these are checked and authorised prior to sending by the Project Manager. See also Paragraphs B9.2 and B9.3 on concerning personal references by management committee members.

#### **D10. Subject access requests**

D10.1 Volunteers are entitled to see their own personal files. To do so, they should arrange a mutually convenient time with the Project Manager.

D10.2 There are certain conditions in which access may be denied: See paragraphs B10.1 and B10.2.

#### **D11. Obligations of volunteers**

See section B11: Obligations of staff and volunteers

#### **D12. Guidelines on disclosing information to internal and external sources**

See section B12: Guidelines on disclosing information to internal and external sources

#### **D13. Organisational information**

See section B13: Organisational information

### **E. Exceptions: breaking confidentiality**

E1. Manningham Project Ltd may break confidentiality if it believes that this is necessary for compliance with a legal obligation or to protect the vital interest of a data subject or another person, including:

- A child is at risk of being harmed
  - A person's life or safety is at risk
  - If required by statute (e.g. there is a legal obligation to report drug trafficking, money laundering, terrorist activity to the police)
  - If required under a contractual obligation (e.g. where services are purchased by a local authority and that contract requires disclosure of certain information)
  - If required by a court order.
- E2. In particular, maintaining the confidentiality of identifiable third parties in the course of a "subject access request" will be considered on a case by case basis.
- E3. In all the above cases, the Project Manager (or if unavailable the Chair or Deputy Chair of Trustees) and, when appropriate the Safeguarding Officer must be informed immediately.
- E4. In other cases where breaking confidentiality may seem appropriate, this must only be done with the knowledge and authorisation of the Project Manager or Trustees and the person whose confidentiality is to be breached must be informed. They should be informed of their right of complaint and appeal.

## **Reviewing**

Adopted 16 January 2012

Reviewed: 9 June 2016

Reviewed: 27 July 2017

Reviewed following new legislation: 19 July 2018

Reviewed to include personal information relating to volunteer: 11 October 2018

Reviewed to include procedure relating to breach of personal data: 2 January 2019

Reviewed by management committee: 18 February 2021

This policy will be reviewed annually.



## **APPENDICES**

Privacy notice for staff

Staff confidentiality statement

Privacy notice for clients

Client consent form

Privacy notice for volunteers

Volunteers confidentiality statement

Procedures relating to personal data breaches



## **Privacy Notice for Staff and Prospective Employees**

### **What is this notice and why are we giving it to you?**

This privacy notice explains what information we need to hold about you and why we do so. It explains how we will use it and protect it and also tells you how you can check it and have it corrected. The Manningham Project is a data controller and is required to give you this notice by the General Data Protection Regulation (GDPR) which came into effect in May 2018. For further detail see the Project's Confidentiality and Data Protection Policy.

### **The reasons we use your personal information**

We only use your personal information as the law allows. Most commonly this is for the following reasons:

1. Where needed for your employment contract with us.
2. Where needed for compliance with our legal obligations.
3. Where needed for legitimate interests of the Manningham Project, but only when these are not overridden by your own interests or fundamental rights.

Other possible reasons are the following, but these are likely to be rare:

1. Where we need to protect your interests, or someone else's.
2. Where it is needed to protect the public interest or for official purposes.

### **The information we hold about you**

Personal information (personal data) 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. We will collect, store and use the following categories of personal information about you:

- Personal contact details including name, title, addresses, telephone numbers and personal email addresses; date of birth; gender; marital status and dependants.
- Recruitment information including: National Insurance number; copies of right to work documents (e.g. passport, immigration status); references and information included in a CV or cover letter as part of the application process; interview dates.
- Work related information including: hours worked; bank details; training records and qualifications obtained; language skills; staff supervision and appraisal records; records concerning complaints, disciplinary or grievance procedures; copy of Disclosure and Barring Service Certificate where needed; information about criminal convictions and offences, where the law allows.
- Special categories of more sensitive information include information about your health, health and sickness records, any medical condition or disability. Information on racial or ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation will only be processed if necessary or advantageous to the employment relationship and with your explicit consent.

### **How we collect and store your personal information**

We collect personal information about staff and prospective employees mainly from the individuals concerned. Sometimes, particularly during recruitment, we may seek information from third parties including employment agencies, former employers, referees, credit reference agencies and or other background check providers and will normally ask your





consent to do so. If concerns arise about occupational health then we may seek independent medical evidence, but only with your explicit consent.

Printed and written information is stored in personnel files in locked filing cabinets accessible only to the Manningham Project Manager. Information processed electronically, such as the for the monthly payroll, is password protected files in the Project's IT system.

### **How we use your information**

We only use your information for the reasons already mentioned. These include making decisions about recruitment and appointment, managing the work you do on behalf of the Project and complying with legal obligations and regulations such as tax laws, health and safety regulations *etc.* We will use information concerning your health, or disability status, to ensure your health and safety in the workplace, to provide workplace adjustments if appropriate and to monitor and manage sickness absence.

We share personal information with third parties only as necessary for administration of your working relationship with us or when required by law. This includes payroll provision, pension administration, IT services (such as AdvicePro), training services, insurers, funding bodies, auditors and regulatory bodies. We will only respond to reference requests about you if we have your written consent.

### **Consent**

We do not generally need your consent provided we use your personal information for the principal reasons stated above. In limited circumstances we may approach you for written consent to use data for another purpose, including those already mentioned, in which case we will provide full details of the information we would like and the reason we need it. In such a case your consent would not be a condition of your contract with us and you would have the right to withhold your consent or to withdraw it at any time.

### **How long do we keep your information?**

We will retain your personal information for as long as needed to fulfil the purposes for which it was collected including satisfying and legal, accounting or reporting requirements. Application and recruitment records are kept for 6 months. Personnel files including training, sickness absence, salary, pay, tax and NI and redundancy will be kept for 6 years after the end of employment.

### **Your rights of access, correction, erasure and restriction**

You have the right to receive a copy of the personal information we hold about you (a *data subject access request*), allowing you to check that it is accurate and that we are holding it legally. You can request incomplete or inaccurate information to be corrected and information to be deleted if there is no good reason for us to hold it. You can also request a restriction to use of your information, for example if you want us to establish its accuracy or the reason for using it. There is normally no fee for exercising these rights.

### **Complaints**

If you have any comment or complaint concerning your information you can speak to the Manager of Manningham Project, who is our official Data Controller, or alternatively to the Chair of Trustees. You can also lodge a complaint with the official regulator, the Data Commissioner's Office. The Manningham Project Limited is registered under the Data Protection Act 1998 to keep personal information electronically and on paper.



## **MANNINGHAM PROJECT LTD STAFF CONFIDENTIALITY STATEMENT**

1. I have read the Manningham Project Privacy Statement for Staff and understand that the organisation will hold and process information about me in line with the Data Protection and Confidentiality Policy and the General Data Protection Regulations.

2. I understand that in the course of my work with Manningham Project Ltd I may learn facts about colleagues or about individuals or organisations with whom Manningham Project Ltd works. I recognise that these facts may be of a personal and confidential nature. I agree not to disclose any such information to any person not authorised by Manningham Project Ltd to hold such information without the express permission of the individual to whom the information pertains, or, in exceptional circumstances, the agreement of my line manager.

3. I agree to uphold this commitment to confidentiality both whilst I am working at Manningham Project Ltd and also in situations outside Manningham Project Ltd

Signed:

Date:

Name (please print):



## Privacy Notice for Clients

### **What is this notice and why are we giving it to you?**

This privacy notice explains what information we need to hold about you and why we do so. It explains how we will use it and protect it and also tells you how you can have it removed from our files if you so wish. We are required to give you this notice by the General Data Protection Regulation (GDPR) which came into effect in May 2018.

### **Your personal information**

The only information we hold is what you tell us so that we can provide the support and advice that you ask for. We will only ask for information that is necessary for our work and we will always ask for your consent. This is the sole legal basis on which we hold your information. Your information is kept securely only in electronic form. It is accessible only to Manningham Project advice workers in the conduct of their work for you and for other legitimate activities of the Manningham Project such as quality assurance and compiling statistical data. We do not share your information with any other organisation or authority unless you have given us explicit permission to do so on your behalf.

### **How long do we keep your information?**

Your information will be kept available for us to use while it is needed in connection with your case. When this work is completed your information is moved into a secure archive where, in case there is any need to revisit your situation, it is kept for six years. It is deleted after six years of non-activity.

### **Quality assurance and statistical data**

Our work is accredited by external quality assurance bodies including the AQS (Advice Quality Standard) and the OISC (Office of the Immigration Services Commissioner). During their quality audits these bodies need to inspect files which include personal information but will only do so if you have given appropriate consent. We also use clients files to compile anonymous statistical information for monitoring and analysing our work and to support applications for funding.

### **Your rights**

You have a legal right to know all the personal information we hold about you. You can ask for this either verbally or in writing through any member of staff and we will respond within a maximum of one month. You can withdraw your consent at any time and can also ask for your information to be erased. If you wish to make any comment or complaint concerning your information you can speak to the Manager of Manningham Project, who is our official Data Controller. You can also lodge a complaint with the official regulator, the Information Commissioner's Office. The Manningham Project Limited is registered under the Data Protection Act 1998 to keep personal information electronically and on paper.



## Client's Consent to Use Personal Information

Name: \_\_\_\_\_

Client ID No. \_\_\_\_\_

Address: \_\_\_\_\_

Date of birth: / /

National Insurance No. \_\_\_\_\_

Please complete the following table by ticking 'Yes' or 'No'. Ticking 'Yes' for items 1 – 4 enables us to carry out the full range of our work for you. You are free to withdraw your consent at any time and to have your information erased should you wish this to be done.

	Yes (✓)	No (✓)
1. Please confirm that you have been given a copy of the client Privacy Statement, which can be used for this and subsequent enquiries.		
2. Do you give consent for the Manningham Project to hold such personal information as needed to provide the support and advice that you are seeking? This may include information about income and expenditure, savings, copies of utility bills, passports, birth certificates, tax records, family details, school attendance and other relevant information. We will only ask for information that is necessary for the work on your behalf.		
3. Some personal information is classed as <b>sensitive</b> for which we need separate consent. This includes information on health, race, ethnicity, religion, and some other areas. We may need this information in our work for you, but some information is also collected for statistical purposes. Do you give consent for the Manningham Project to hold sensitive information when it has legitimate reasons to do so?		
4. Do you give consent for the Manningham Project to discuss your personal information with third parties when you have agreed that we may do so on your behalf?		
5. Do you give your consent for your file to be inspected during quality audits by accreditation bodies? These bodies do not retain personal information after their inspection.		
6. We will erase all electronic files securely after six years of non-activity.		

Please sign below to confirm the responses you have given.

Signed \_\_\_\_\_



## **Privacy Notice for Volunteers and Prospective Volunteers**

### **What is this notice and why are we giving it to you?**

This privacy notice explains what information we need to hold about you and why we do so. We are required to give you this by the Data Protection Act 2018.

### **The information we need**

We will hold only such information about you as required for the purposes of recruitment and selection and for managing your activities while working with us as a volunteer. This will include:

- Personal contact details including name, title, addresses, telephone numbers and personal email addresses, date of birth, gender.
- Recruitment information including references and information included in a CV or cover letter as part of the application process. Other relevant information might include: qualifications obtained, language skills, copy of Disclosure and Barring Service Certificate where needed, information about criminal convictions and offences where the law allows.
- More sensitive information might include information about your health and any medical condition or disability. We would only use this to ensure your health and safety in the workplace.

We will also maintain records of your volunteer activities undertaken at the Manningham Project and of related supervision meetings.

### **Your consent**

As you are volunteer we only legally hold your information based on your written consent.

### **How we collect and store your personal information**

You will always be the primary source for any information we have about you. During recruitment we will also seek information from your referees but only when we have your consent to do so. Information is kept in confidential files in locked filing cabinets accessible only to the Manningham Project Manager and will be provided only to other appropriate members of staff within the organisation. Emails and telephone contact details may be held in password protected IT systems.

### **How long do we keep your information?**

If your application is successful we will retain your personal information while you are either actively volunteering or you have told us that you are available to volunteer. We may keep information for up to six years after you cease to be a volunteer, in line with our standard personnel policy. If your application is unsuccessful we will securely erase your information within one month.

### **Your rights**

You have the right to receive a copy of the personal information we hold about you, to request inaccuracies to be corrected and information to be deleted if there is no good reason for us to hold it. If you have any comment or complaint concerning your information you can speak to the Manager of Manningham Project, who is our registered Data Controller, or alternatively to the Chair of Trustees. You can also lodge a complaint with the official regulator, the Data Commissioner's Office. The Manningham Project Limited is registered under the Data Protection Act 1998 to keep personal information electronically and on paper.



## Volunteer's Consent and Confidentiality Statement

Name: \_\_\_\_\_

Address:

---

### A. Consent to Use Personal Information

(Complete on application)

I have read the Manningham Project Privacy Statement for Volunteers and I give my consent for the organisation to hold information about me in line with the Project's Data Protection Policy and with the Data Protection Act 2018.

Signed:

Date:

---

### B. Confidentiality Statement

(Complete during induction)

1. I understand that in the course of my work with Manningham Project Ltd I may learn facts about colleagues or about individuals or organisations with whom Manningham Project Ltd. works. I recognise that these facts may be of a personal and confidential nature. I agree not to disclose any such information to any person not authorised by Manningham Project Ltd. to hold such information without the express permission of the individual to whom the information pertains, or, in exceptional circumstances, the agreement of my line manager.
2. I agree to uphold this commitment to confidentiality both whilst I am working at Manningham Project Ltd. and also in situations outside Manningham Project Ltd.
3. I have read and understood the Manningham Project Data Protection Policy.

Signed:

Date:



## Procedures Relating to Personal Data Breaches

1. A personal data breach refers to a breach of security leading to the accidental or unlawful *destruction, loss, alteration, unauthorised disclosure of, or access to*, personal data.
2. Any incident or circumstance resulting in either significant risk of a breach of security of any personal data or in an actual breach must be reported to the Project Manager and recorded in the Project's incident book.
3. The Project Manager will determine what further action, if any, is appropriate including:
  - informing the chair of trustees
  - action to prevent consequential adverse effects
  - action to mitigate or avoid further breaches
  - notify the Information Commissioners Office (ICO), if necessary (see below)
  - notify affected individuals, if necessary (see below).
4. When it is necessary to inform the ICO
  - The ICO must be notified about any breach that is *likely* to result in a risk of adverse effects for any individuals. Adverse effects might include loss of control over personal data, discrimination, identity theft, financial loss, damage to reputation, emotional distress or any significant economic or social disadvantage.
  - The ICO should be notified without undue delay and not later than 72 hours after becoming aware of the breach. For information on notifying the ICO see: <https://ico.org.uk/for-organisations/report-a-breach/>.
  - It is *not* necessary to inform the ICO if a risk of adverse effects is *unlikely*. A decision not to inform the ICO should be agreed by the chair of trustees and must be documented with the reasons justifying the decision. Failure to notify the ICO when required to do so can result in a significant fine.
5. When it is necessary to inform affected individuals
  - Individuals must be notified if a breach is likely to result in a *high risk* of an adverse effect. This should be done directly and as soon as possible.
  - The threshold for informing individuals (a 'high risk') is higher than for informing the ICO. The risk depends on both the *severity* of the potential or actual impact and on the *likelihood* of this occurring. If either the potential severity or the likelihood is considered high then affected individuals should be informed promptly, particularly if this will help individuals to take steps to protect themselves from the breach.
  - A decision not to inform affected individuals should be agreed by the chair of trustees and must be documented with the reasons justifying the decision. Failure to notify individuals when required to do so can result in a significant fine as well as the risk of civil action and the loss of the Project's reputation.

This appendix is based on the 'Personal data breaches' section of the ICO's online *Guide to the General Data Protection Regulation* (<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>, accessed January 2019).