Manor House Development Trust (MHDT)
Data Protection & Confidentiality Policy

General principles

1 Personal data will be processed lawfully and fairly

1.1 Data will not be processed fairly and lawfully unless:

1.1.1 in the case of data obtained from the individual himself, MHDT will provide or make readily available to the individual, certain specified information (see 1.2); and

1.1.2 in any other case, e.g. where data is obtained from a third party, MHDT will provide or make readily available to the individual certain specified information (see 1.2).

1.2 The information to be provided or made available is:

1.2.1 the identity of the organisation;

1.2.2 the purpose(s) for which the data are processed; and

1.2.3 any further information which in the circumstances is necessary to ensure compliance with the first data protection principle.

2 Compliance

2.1 In order to comply with this Principle, data processing must meet **at least one** of the following conditions:

2.1.1 The individual has given their consent to the processing;

2.1.2 The existence or validity of consent will need to be assessed in light of the facts. Consent is not defined in the Act but the Data Protection Directive from which the legislation emanated defines 'consent' as:

'... any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'.

2.2 Even where consent has been given it will not necessarily last forever. An individual must be able to withdraw their consent; equally, consent for one type of data processing may not apply to a new, different type of processing.

2.2.1 The processing is necessary:

2.2.1.1 for the performance of a contract to which the individual is a party, or

2.2.1.2 for the taking of steps at the request of the individual with a view to entering into a contract.

2.2.2 The processing is necessary to comply with any legal obligation to which the organisation is subject, other than an obligation imposed by contract.

2.2.3 The processing is necessary in order to protect the vital interests of the individual. (The ICO considers that reliance on this condition may only be claimed where the processing is necessary for matters of life and death, for example, the disclosure of an individual's medical history to a hospital Casualty Department treating the individual after a serious road accident.)

2.2.4 The processing is necessary for:

2.2.4.1 the administration of justice;
2.2.4.2 the exercise of any functions conferred by or under any enactment (i.e. functions conferred by law);
2.2.4.3 the exercise of any functions of the Crown, a Minister of the Crown or a government department; or
2.2.4.4 the exercise of any other functions of a public nature exercised in the public interest.

2.2.5 The processing is **necessary** for the purposes of legitimate interests pursued by the organisation or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the individual.

3 Purposes of data collection

3.1 Personal data may only be obtained for one or more specified and lawful purposes and may not be further processed in any way incompatible with that or those purposes.

3.2 There are two ways in which an organisation may specify the purposes:

3.2.1 in a notice to the individual;
3.2.2 in a notification given to the ICO.

3.3 In deciding whether any disclosure of personal data is compatible with the purposes, consideration will be given to the purposes for which the personal data are intended to be processed by any person to whom they are disclosed.

4 Adequate, relevant and not excessive

4.1 Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.

4.2 MHDT will communicate the purpose of personal data collection and ensure by continuous monitoring that the data processed relates directly to those purposes and, where necessary, remove excessive or unwanted data.

5 Maintaining accurate and up to date information

5.1 This principle will not be regarded as contravened by reason of any inaccuracy in data which have been accurately recorded by MHDT where:

5.1.1 having regard to processing purpose(s), MHDT has taken reasonable steps to ensure the accuracy of the data; and
5.1.2 if the individual tells MHDT that the data are inaccurate, the data indicate that fact.

6 Not keeping data for longer than necessary

6.1 MHDT will review all data regularly and delete anything that is no longer necessary. Data will be retained where it is still needed to fulfil the original purpose.

7 Processing

7.1 Personal data must be processed in accordance with the rights of data subjects under the Data Protection Act.

7.2 MHDT will contravene this principle if:

7.2.1 it fails to provide the subject access information requested by an individual;
7.2.2 it fails to comply with a notice requiring it to stop, or not to begin, processing personal data relating to him/her for a specified purpose or in a specified manner, on the ground that it will cause substantial damage or substantial distress.

7.1 MHDT will put in place appropriate measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. This includes:

7.1.1 Taking reasonable steps to ensure the reliability of any employees who have access.
7.1.2 Where MHDT uses an external data processor, e.g. a payroll services organisation, MHDT will choose an external data

processor that can provide sufficient guarantees in respect of security measures in place, and must take reasonable steps to ensure compliance with those measures.

8 Sensitive personal data

8.1 MHDT agrees to comply with at least one of the following conditions:

8.1.1 The individual has given explicit consent to the processing of the personal data.

8.1.2 The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the organisation in connection with employment.

8.1.3 The processing is necessary:

8.1.3.1 in order to protect the vital interests of the individual or another person, in a case where;

8.1.3.1.1 consent cannot be given by or on behalf of the individual; or

8.1.3.1.2 the organisation cannot reasonably be expected to obtain the consent of the individual; or

8.1.3.2 in order to protect the vital interests of another person, in a case where consent by or on behalf of the individual has been unreasonably withheld.

8.1.4 The processing is carried out in the course of its legitimate activities by any association which is not established or conducted for profit, and

8.1.4.1 exists for political, philosophical, religious or trade union purposes;

8.1.4.2 is carried out with appropriate safeguards for the rights and freedoms of individuals;

8.1.4.3 relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes; and

8.1.4.4 does not involve disclosure of the personal data to a third party without the consent of the individual.

8.1.5 The information contained in the personal data has been made public as a result of steps deliberately taken by the individual.

8.1.6 The processing:

8.1.6.1 is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
8.1.6.2 is necessary for the purpose of obtaining legal advice, or
8.1.6.3 is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

8.1.7 The processing is necessary:

8.1.7.1 for the administration of justice;
8.1.7.2 for the exercise of any functions conferred on any person by or under an enactment; or
8.1.7.3 for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

8.1.8 The processing is necessary for medical purposes and is undertaken by:

8.1.8.1 a health professional; or
8.1.8.2 a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

8.1.9 The processing:

8.1.9.1 is of sensitive personal data consisting of information as to racial or ethnic origin;
8.1.9.2 is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and
8.1.9.3 is carried out with appropriate safeguards for the rights and freedoms of individuals.

8.1.10 The personal data are processed in circumstances specified in an order made by the Secretary of State.

9 Access to information

9.1 Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the employee dealing with the case and their line manager. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled

to access the information and the name of the individual or group who may request access to the information.

9.2 Employees may have sight of their personnel records by giving 14 days' notice in writing to the Director.

9.3 Users may have sight of records held in their name or that of their organisation. The request must be in writing to the Director giving 14 days' notice and be signed by the individual, or in the case of an organisation's records, by the Chair or Executive Officer. Sensitive information as outlined in para 3.2 will only be made available to the person or organisation named on the file.

10 Storing / transporting information

10.1 General non-confidential information about organisations is kept in unlocked filing cabinets with open access to all (GROUP) colleagues.

10.2 Information about volunteers, interns and other individuals will be kept in filing cabinets by the colleague directly responsible. These colleagues must ensure line managers know how to gain access.

10.3 Employees' personnel information will be kept in lockable filing cabinets by line managers and will be accessible to the Director.

10.4 Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.

10.5 In an emergency situation, the Director may authorise access to files by other people.

10.6 When photocopying or working on confidential documents, colleagues must ensure they are not seen by people in passing. This also applies to information on computer screens.

11 Duty to disclose information

11.1 There is a legal duty to disclose some information including:

11.1.1 Child abuse will be reported to the Children's Services Department

11.1.2 Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.

11.1.3 Colleagues believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the Director who will report it to the appropriate authorities.

11.2 Users should be informed of this disclosure.

12 Disclosures

12.1 MHDT complies fully with the CRB Code of practice regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.

12.2 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a criminal offence to pass this information to anyone who is not entitled to receive it.

12.3 Documents will be kept for a year and then destroyed by secure means. Photocopies will not be kept. However, (GROUP) may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, and the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

13 Breach of confidentiality

13.1 Colleagues accessing unauthorised files or breaching confidentially may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

14 Confidentiality

14.1 MHDT recognises that colleagues (employees, volunteers, interns, trustees) gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, employees must seek advice from their line manager.

14.2 Colleagues are able to share information with their line manager in order to discuss issues and seek advice.

14.3 Colleagues should avoid exchanging personal information about individuals with whom they have a professional relationship.

14.4 Colleagues should avoid talking about organisations or individuals in social settings.

14.5 Colleagues will not disclose to anyone, other than their line manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.