DATA PROTECTION

OUTCOMES

Colleagues will be aware of, understand and know how to implement the Data Protection Act, the General Data Protection Regulation and the Privacy of Electronic Communications Regulation when processing personal data.

SCOPE

This policy applies to MHA where a Data Subject's personal data is processed:

a. By MHA Colleagues (including while away from work).

b. In the context of the business activities of MHA.

c. For the provision of goods or services to individuals (including those provided or offered free-of-charge) by MHA.

d. To actively monitor the behaviour of individuals.

This policy applies to all processing of personal data in electronic form (including electronic mail and documents) or where it is held in manual files that are structured in a way that allows ready access to information about individuals.

This policy has been designed to establish a baseline for the processing and protection of personal data by MHA. Where national law imposes a requirement, which is stricter than imposed by this policy, MHA must follow the requirements in national law. Furthermore, where national law imposes a requirement that is not addressed in this policy, MHA must adhere to the relevant national law.

If there are conflicting requirements in this policy and national law, please contact MHA's DPO.

1. INTRODUCTION

See also IG002a, Data Protection - Definitions

1.1. Methodist Homes (MHA) is committed to conducting its business in accordance with all applicable Data Protection Legislation (the Legislation).

1.2. This policy sets out the expected behaviours of MHA Colleagues and Third Parties in relation to the collection, use, retention, transfer, disclosure and destruction of any personal data belonging to an Identifiable Natural Person, the Data Subject.

1.3. Personal data is any information (including opinions and intentions) which relates to a Data subject. The Legislation impose restrictions on how organisations may process personal data. An organisation that handles personal data and makes decisions about its use is known as a Data Controller. MHA, as a Data Controller, is responsible for

ensuring compliance with the Legislation as outlined in this policy. Non-compliance may expose MHA to complaints, regulatory action, fines and/or reputational damage.

1.4. MHA's CEO and leadership team is fully committed to ensuring continued and effective implementation of this policy, and expects all MHA Colleagues and Third Parties to share in this commitment. Any breach of this policy will be taken seriously and may result in disciplinary action or business sanction.

1.5. The Legislation does not relate to records of the deceased. Access to health records of the deceased is governed by the "Access to Health Records Act (1990) which states:

3. (1) An application for access to a health record, or to any part of a health record, may be made to the holder of the record by any of the following,

(a) the patient; …

(f) where the patient has died, the patient's personal representative and any person who may have a claim arising out of the patient's death.

2. GOVERNANCE

2.1. Data Controller

MHA is the Data Controller for most of the personal data processed by MHA. MHA is responsible to make sure that it applies the Legislation throughout the business and can prove compliance to the Information Commissioner's Office (ICO).

MHA may enter in contracts with third parties - e.g. local authorities, Clinical Commissioning Groups - to provide a service on their behalf. In most case MHA and the third party will be processing the personal data for different purposes, though the purpose may be related. The parties will be independent Data Controllers. There may be instances where MHA and the third party are jointly determining the purpose and what information needs to be processed. Under these circumstances the two parties will be Joint Data Controllers. A contract between Joint Data Controllers is required to specify:

- The respective responsibilities of both parties.
- The respective roles regarding the data subjects.
- Who the data subject should contact in regards of each controller.

Any contract referring to MHA as a Joint Controller must be reviewed by the DPO before signing.

2.2. Data Processors

MHA may engage with the external bodies to carry out some processing on behalf of MHA. All such processing will be governed by a contract to make sure that:

a. The data is only processed for the purposed requested by MHA.

b. The data will not be shared with any other party.

c. The data processor is compliant to the Legislation.

d. MHA's data will be returned to MHA when the contract ends and all copies held by the contractor will be destroyed.

2.3. Data Protection Officer

As required by the Legislation, MHA has a Data Protection Officer (DPO). The DPO operates with independence and is granted all necessary authority. The DPO reports to MHA's Company Secretary who is a member of MHA's Executive Leadership Team and has direct access to MHA's Board of Directors. The DPO's duties include:

a. Advising MHA and its Colleagues regarding the processing of data in accordance with the Legislation.

b. Providing guidance with regards to carrying out Data Protection Impact Assessments (DPIAs).

c. Recording all incidents involving personal data and determining when the ICO and/or data subjects need to be informed of a breach.

d. Data Protection compliance monitoring.

e. Ensuring the establishment of procedures and contractual provisions with third parties as necessary.

2.4. Quality Assurance Monitoring

The DPO will carry out a Data Protection quality assurance audits for all locations and departments to determine the level of compliance (**see IG011**). Each audit will, as a minimum, assess:

a. Application of the Legislation's principles

b. Staff awareness and training

c. Processing of Data Subject's rights, including the involvement of the DPO

d. Incident and breach reporting to the DPO

The DPO, in cooperation with key business stakeholders, will devise a plan with which to correct any identified deficiencies within a defined and reasonable time frame. MHA's Leadership Team will be informed of any major deficiencies.

2.5. Policy Dissemination & Enforcement

MHA's Leadership Team must make sure that all MHA colleagues responsible for the processing of personal data are aware of and comply with the contents of this policy.

In addition, MHA must make sure all third parties engaged to process personal data on their behalf, i.e. their Data Processors, are aware of and comply with the contents of this policy. Assurance of such compliance must be obtained from all third parties in writing, whether companies or individuals, prior to granting them access to personal data controlled by MHA.

2.6. Data Protection by Design

Data Protection by Design requires that all risks involving personal data are considered when:

a. new systems are being considered and implemented.

b. changes are being made to systems affecting the use of personal data.

c. security or access criteria are being changed.

d. business processes involving personal data are changed.

e. Data is being transferred outside the UK.

Each of these projects or changes must go through an approval process before continuing.

The approval process is carried out by a Data Protection Impact Assessment (DPIA). All colleagues involved in such changes involving: systems, reports, processes or access to systems and data must engage with the DPO, the Change Team or the IT Department who will assist with the DPIA. The subsequent findings of the DPIA must then be reviewed and approved.

3. DATA PROTECTION PRINCIPLES

MHA must apply the following principles when processing personal data:

Principle 1: Lawfulness, Fairness and Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the Data subject.

MHA must tell the Data subject, through Privacy Notices (transparency), what data will be processed and how it will be processed (fairness), the legal basis for the processing - e.g. contract, consent (opt-in) or Legitimate Interest (opt-out) (lawfulness).

Principle 2: Purpose Limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

MHA must specify exactly what the personal data collected will be used for and limit its use to the specified purpose.

Principle 3: Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

MHA must only process data that is necessary to carry out the task for which the data is being held.

Principle 4: Accuracy

Personal data must be accurate and, kept up to date.

MHA must have in place procedures for identifying and addressing out-of-date, incorrect and redundant personal data.

Principle 5: Storage Limitation

Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

MHA must have retention policies (see IG001a) in place to specify when data is to be deleted and procedures to ensure the data is deleted when necessary.

Principle 6: Integrity & Confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

MHA must use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained.

Principle 7: Accountability

The Data Controller must be responsible for, and be able to demonstrate compliance.

MHA must be able to demonstrate that the six Data Protection Principles are being applied though detailed policies, procedures, training and regular audits.

3.1. The Legal Basis for Processing Personal Data

There are six legal bases for the processing of personal data:

a. The data subject has provided **consent**. Note that consent can be revoked.

b. It is necessary for the **performance of a contract** - e.g. employment.

c. Compliance with a **legal obligation** - e.g. disclosing salary information to the HMRC.

d. Protection of the **vital interests** of the data subject - e.g. providing medical information in a life threatening situation.

e. Carrying out a task in the **public interest** - e.g. using CCTV for crime prevention.

f. **Legitimate interest** of MHA - e.g. using photos taken at a public event or sending fundraising and marketing information via post where the individual has not opted out of receiving the information.

a. Data Subject Consent

MHA will obtain personal data only by lawful and fair means and, where appropriate with the knowledge and consent of the individual concerned. Where MHA is relying on consent as the basis for processing personal data, MHA will request, receive and record the consent before or at the point of collection.

The business stake holder, in cooperation with the DPO, must establish a system for obtaining and documenting the consent. The system must include provisions for:

a. Determining what additional information is required to record valid consent, i.e. so the person giving consent can be identified. E.g. name, address, phone number and email address as appropriate.

b. Ensuring the request for consent is clearly distinguishable from any other matters, can easily be given, and uses clear and plain language.

c. Ensuring the consent is freely given.

d. Documenting the date, method (including the ability to retain paper forms or digital copies of the forms) and identifying details, as well as the scope of the consents given.

e. Providing a simple method for a data subject to withdraw their consent at any time.

When the data subject is asked to give consent to the processing of their personal data and the personal data is collected from the data subject a Privacy Notice must be provided.

Consent may be given verbally, electronically or in writing. If given verbally, the person taking the details must record the consent, e.g. by using the Verbal Record Form (**IG002b**). The form must be retained to prove the conversation.

b. Performance of a Contract

All contracts created by MHA must ensure that the six principles are being adhered to, see Data Protection Principles.

When a resident moves into a service under a contract, e.g. Local Authority or CCG, the contract typically grants an authorised official the right to access the resident's records. This includes requesting copies of those records. It is the responsibility of the home / scheme manager to know which residents are placed under contract and to manage access to the records for the designated officials.

c. Legal and Statutory Requirement

MHA will comply with all legal and statutory requirements. MHA will include details in relevant Privacy Notices.

d. Protection of Vital Interests

In an emergency situation MHA may engage with family members, medical professionals, etc. in order to protect the life of data subjects. Where residents have a Do Not Resuscitate Order on file this will take precedence.

e. Tasks carried out for Public Interest

MHA may carry out tasks for Public Interest. These will typically be: safeguarding, the use of CCTV for crime prevention and the tracking of IP addresses to ensure that no illegal activity is carried out by individuals using IT services offered by MHA - e.g. business or free internet access.

f. Legitimate Interest

Whenever the legal basis of Legitimate Interest is being considered a Legitimate Interest Assessment, (**IG002c**) must be completed and returned to the DPO. The DPO will record the assessment in the data protection logs and provide a decision on whether it is reasonable to use Legitimate Interest. It must be noted that though MHA may have a legitimate interest to process the data this is not sufficient - there are additional tests that need to be carried out before a decision can be made.

Examples of MHA's use of legitimate interest includes:

- MHA will share employee details with the Rewards Gateway. This is not required for employment but MHA considers it a legitimate interest of MHA to provide these benefits.

- MHA may take photos or videos at events which will capture individuals. The use of these photos or videos will be for legitimate business interests of MHA and are not expected to significantly affect the rights and freedoms of those caught on film.

Where communications to individuals are made on the basis of legitimate interest (after a legitimate interest assessment has been completed) that communication must include detail on the right to opt-out of communications and the means by which to make the

request, e.g. an email address or phone number. On opt-out must be actioned with 1 calendar month.

g. Processing Special Categories of Data

MHA will only process Special Categories of Data (also known as sensitive data) where one of the following conditions apply:

a. There is a contract in place covering the processing, e.g. employment contract, care contract.

b. The data subject has provided consent, e.g. privately funded residents and MHA Communities members.

c. The processing relates to personal data which has already been made public by the data subject.

d. The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.

e. The processing is authorised or required by law or an exception under the Legislation.

In any situation where Special Categories of Data are to be processed, prior approval must be obtained from the DPO and the basis for the processing clearly recorded with the personal data in question.

Where Special Categories of Data are being processed, MHA will ensure that suitable protection measures are in place to protect the data.

As required by the Data Protection Act 2018 (Schedule 1 Part 4) MHA has in place the required Appropriate Policy Document (**IG002d**) covering the processing of Special Category and Criminal Offence data. This will be updated from time to time and is available on MHA's intranet and website (www.mha.org.uk/PrivacyPolicy).

3.2. Privacy Notices

MHA will make available Privacy Notices covering the processing of personal data, see **IG003**, Data Subject Rights.

3.3. Cookies

MHA will provide an online 'Cookie Notice' and preference page for each website made available by MHA as required by the Legislation.

All Cookie Notices and preference settings must be approved by the DPO prior to use or publication on an external website.

4. DATA PROCESSING

4.1. Data Collection

Personal data should only be collected from the data subject unless one of the following apply:

a. The nature of the business purpose necessitates collection of the personal data from other persons or bodies - e.g. contract with Local Authority or Clinical Commissioning Group.

b. The collection must be carried out under emergency circumstances in order protect the vital interests of the data subject - e.g. from a family member or General Practitioner.

c. If personal data is collected from someone other than the data subject, the data subject must be informed of the collection unless one of the following apply:

- The data subject has received the required information by other means.
- The information must remain confidential due to a professional or legal obligation.
- A national law expressly provides for the collection, processing or transfer of personal data.
- Where it has been determined that notification to a data subject is required, notification must occur promptly, but in no case later than:

  - One calendar month from the first collection or recording of the personal data.
  - At the time of first communication if used for communication with the data subject.
  - Prior to disclosure if it is to be disclosed to another recipient.

4.2. Using Personal Data

MHA uses personal data for the following purposes:

a. The administration of MHA's responsibilities as an employer.

b. The general running and business administration of MHA.

c. To provide services to people using MHA's services.

d. The ongoing administration and management of customer services.

e. MHA's supporter activities.

f. Direct marketing and fundraising

The use of personal information should always be considered from the data subject's perspective and whether the use will be within their expectations or if they are likely to object. For example, it would clearly be within a person's expectations that their details will be used by MHA to respond to a request for information about the products and

services they have enquired about. However, it will not be within their reasonable expectations that MHA would use or share their details for marketing purposes.

MHA will process personal data in accordance with the Legislation and applicable contractual obligations. More specifically, MHA will not process personal data except as detailed by 'The Legal Basis for Data Use'.

There are some circumstances in which personal data may be further processed for purposes that go beyond the original purpose for which the personal data was collected. When deciding as to the compatibility of the new reason for processing, guidance and approval must be obtained from the DPO before any such processing may commence.

a. Data Quality

MHA will adopt all necessary measures to ensure that the personal data it collects and processes is complete and accurate in the first instance, and is updated to reflect the current situation of the data subject. The measures adopted by MHA to ensure data quality include:

a. Correcting personal data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the data subject does not request rectification.

b. Keeping personal data only for the period necessary to satisfy the permitted uses or applicable statutory retention period.

c. The removal of personal data if in violation of any of Data Protection principles or if the personal data is no longer required.

d. Restriction, rather than deletion of personal data, insofar as:

e. a law prohibits erasure.

f. erasure would impair legitimate interests of the data subject, e.g. the need to keep a record of their opt-out of postal communications.

g. the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

4.3. Direct Marketing including Fundraising

Direct marketing covering any marketing that is sent to a targeted, named individual. It does not include partial addressed marketing (i.e. services that send marketing material to bulk addresses in a postal area addressed to 'The Occupier' or similar) or door drops when the marketing is not addressed to the individual.

Marketing also includes advertising the services that MHA offer, engaging with supporters to promote MHA and all aspects of fundraising.

In addition to the Data Protection Act and the UK GDPR, the Privacy and Electronic Communications Regulations (PECR) must be adhered to when sending marketing material electronically, e.g. via email or text.

a. The Legal Basis for Direct Marketing

Promoting MHA and Fundraising

On 1 May 2021 MHA changed the legal basis for direct marketing (excluding property sales) via postal services and telephone from **consent** to **legitimate interest**. This means that people who gave consent, for direct marketing, before the change date must have their choices honoured. Where consent was declined (i.e. not given – the box was not ticked) this does not mean that we can rely on legitimate interest. The legal basis can only be changed if communication is received which provides an update to their preferences, e.g. a new response form that specifies postal marketing will be sent until they opt-out of receiving it.

NOTE: Legitimate interest only applies to post and telephone marketing and fundraising. Consent is still required for email and text communications that include marketing and fundraising.

Where a new use of personal data for marketing is being considered a Legitimate Interest Assessment must be completed and returned to the DPO. It cannot be assumed that a previous decision to use legitimate interest applies to the new processing.

Property Sales

The legal basis for market of property is consent. The consent will be recording in the Sales Department's Customer Relationship Management (CRM) system.

b. Digital Marketing

MHA will not send promotional or direct marketing material through digital channels such as mobile phones, email and the Internet, without first obtaining consent as required by PECR.

Where consent has been given to use personal data for digital marketing purposes, the data subject must be informed at the point of first contact that they have the right to change their mind or object to having their data processed for such purposes. If the data subject puts forward an objection to digital marketing, processing of their personal data must cease immediately. The records must be updated to reflect their opt-out decision, rather than being completely deleted.

It should be noted that where digital marketing is carried out in a 'business to business' context, there is no legal requirement to obtain consent, provided the person is given the opportunity to opt-out and is in a role related to the marketing.

4.4. Children's Data

Children are **not** able to consent to the processing of their personal data. Consent must be sought from the person who holds parental responsibility over the child. However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

All proposed processing of children's date must be discussed with the DPO. An example of where we would need to process consent is the use of photos or video footage where a child is included.

4.5. Profiling & Automated Decision-Making

MHA will only engage in profiling and automated decision-making where explicit consent has been given or where it is necessary for the performance of a contract with the data subject or where it is authorised by law.

Where MHA utilises profiling and automated decision-making, this will be disclosed to the relevant data subjects. In such cases the data subject will be given the opportunity to:

a. Express their point of view.

b. Obtain an explanation for the automated decision.

c. Review the logic used by the automated system.

d. Supplement the automated system with additional data.

e. Have a human carry out a review of the automated decision.

f. Contest the automated decision.

g. Object to the automated decision-making being carried out.

MHA must also ensure that all profiling and automated decision-making relating to a data subject is based on accurate data.

5. CCTV

MHA uses CCTV system for crime prevention and detection. To comply with data protection law and the Information Commissioner's Code of Practice all sites with a CCTV system installed **must**:

a. only use the system for crime prevention and detection - i.e. not watching staff unless it relates to a crime.

b. make sure the videos only cover MHA property - i.e. not roads, paths or property outside our boundaries.

c. have signs (yellow with CCTV image in a triangle) in visible location stating:

   - Methodist Homes is the Data Controller. It is OK to have Methodist Homes (MHA) but not just MHA.
   - The system is used for crime detection and prevention.
   - The contact telephone number is 01332 221893 / 01332 296200.

d. be password protected with need to know access.

e. have monitors turned off when not being used.

f. record with a quality such that faces and vehicle registration numbers can be identified.

g. have a process for extracting sections of the recording with all personal data not relating to the data subject being blurred - e.g. other faces, children, vehicle registration numbers.

h. have recording restricted to a rolling 30 days.

6. DATA RETENTION

To ensure fair processing, personal data will not be retained by MHA for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

The length of time for which MHA needs to retain personal data is set out in MHA's 'Data Retention Schedule' (**IG001a**). This takes into account the legal and contractual requirements, both minimum and maximum, that influence the retention periods set forth in the schedule. All personal data must be deleted or destroyed as soon as possible where it has been confirmed that there is no longer a need to retain it.

7. PROTECTING THE DATA

MHA will adopt physical, technical, and organisational measures to ensure the security of personal data. This includes the prevention of loss or damage, unauthorised alteration, access or processing, and other risks to which it may be exposed by human action or the physical or natural environment.

The minimum set of security measures to be adopted by MHA is provided in the MHA 'Information Security Policy' (**IG007**).

8. DATA SUBJECT RIGHTS

The DPO will responsible for facilitating data subject rights to exercise their rights:

a. Right to be informed

b. Right of access

c. Right to rectification

d. Right to erasure

e. Right to restrict processing

f. Right to data portability

g. Right to object

h. Rights in relation to automated decision making and profiling.

All requests for Right of Access (or Subject Access Request) must be directed to the DPO. Each request will be logged as it is received. Appropriate verification must confirm that the requestor is the data subject or his / her authorised legal representative. A complete response to each request must be provided within one calendar month of the receipt of the identity verification or the date the request was received from the data subject, if no identity verification is required. If the request is made electronically the information will be provided electronically unless otherwise requested.

For more information see **IG003**, Data Subjects' Rights.

9. COMPLAINTS HANDLING

In addition to the data subject's rights, data subjects with a complaint about the processing of their personal data, may put forward the matter in writing to the DPO or the Information Commissioner's Office.

An investigation of the complaint will be carried out. The DPO or Information Commissioner's Officer will inform the data subject of the progress and the outcome of the complaint within one calendar month.

10. REPORTING OF POLICY BREACHES

All security incidents possibly involving personal data must be reported to the DPO, by email (the DPO's personal email address or DataProtectionOfficer@mha.org.uk) or phone (01332 221 893 or 077916 216 46), the same day the incident is identified.

For more information see the Information Incident Reporting Policy (IG004).

11. DATA PROTECTION TRAINING

All MHA Colleagues that have access to personal data will have their responsibilities under this policy outlined to them as part of their induction training. In addition, MHA will provide regular data protection training and procedural guidance.

12. DATA TRANSFERS

MHA may transfer personal data to internal departments or third-party recipients located in UK or another country where that country is recognised as having an adequate level of legal protection for the rights and freedoms of the relevant data subjects. Where transfers need to be made to countries lacking an adequate level of legal protection, they must be made in compliance with an approved security framework or covered by Standard Contractual Clauses.

12.1. Transfers between MHA Entities

For MHA to carry out its operations effectively across its various locations there may be occasions when it is necessary to transfer personal data from one MHA location to another. Should this occur, MHA remains responsible for ensuring protection for that personal data. When transferring personal data to another MHA location:

- Only transfer the minimum amount of personal data necessary for the purpose of the transfer (for example, to fulfil a transaction or carry out a particular service).

- Ensure adequate security measures are used to protect the personal data during the transfer (including encryption or sign-for post, where necessary).

12.2. Transfers to Third Parties

MHA will only transfer personal data to, or allow access by, third parties when it is assured that the information will be processed legitimately and protected appropriately by the recipient. Where third party processing takes place, MHA will first identify if, under applicable law, the third party is considered a Data Controller or a Data Processor of the personal data being transferred.

All third party transfers, to a Data Controller or Data Processor, must be covered by an appropriate contract to clarify each party's responsibilities in respect of the personal data transferred. MHA has an Information Sharing Policy (**IG009**) which colleagues must follow.

The DPO may conduct audits, as allowed by the Legislation, to ensure the processing is compliant with the contract and the Legislation.

13. POLICY MAINTENANCE

All enquiries / queries about this policy, including requests for exceptions or changes must be directed to the DPO's personal email address or DataProtectionOfficer@mha.org.uk.

14. RELATED DOCUMENTS

Listed below are documents that relate to and are referenced by this policy.

- Information Governance Policy
- Information Incident Reporting Procedure
- Subject Rights Procedure
- Privacy by Design
- Confidentiality Policy
- Information Security Policy
- Document and Records Management Policy
- Information Sharing Policy
- Archiving Policy