DATA PROTECTION

1. INTRODUCTION

1.1 Methodist Homes (MHA) is committed to conducting its business in accordance with all applicable Data Protection laws and regulations (General Data Protection Regulation (GDPR) & Data Protection Bill (DPB)) and in line with the highest standards of ethical conduct.

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 the Data subject. Personal data is subject to certain laws, which 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 data protection requirements 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 GDPR and the DPB do not relate to records of the deceased (see Recital 27). 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. SCOPE

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

- By MHA Colleagues (including while away from work).
- In the context of the business activities of MHA.
- For the provision of goods or services to individuals (including those provided or offered free-of-charge) by MHA.
- To actively monitor the behaviour of individuals.

2.2 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.

2.3 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.

2.4 If there are conflicting requirements in this policy and national law, please contact MHA's Data Protection Officer.

3. GOVERNANCE

3.1 Data Controller

MHA is the Data Controller for all personal data processed by MHA. MHA is responsible to make sure that it applies the GDPR throughout the business and can prove compliance to the UK's Statutory Authority, 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. This may lead to MHA determining what information needs to be processed and determining the way that it is processed. Under these circumstances the two parties will be joint Data Controllers. A contract 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.

3.2 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:

- The data is only processed for the purposed requested by MHA.
- The data will not be shared with any other party.
- The data processor is compliant to the GDPR.
- MHA's data will be returned to MHA when the contract ends and all copies held by the contractor will be destroyed.

3.3 Data Protection Officer

As required by the GDPR MHA has a Data Protection Officer (DPO). The DPO operates with independence and is suitability skilled and granted all necessary authority. The DPO reports to MHA's Director of Quality who is a member of MHA's Leadership Team and has direct access to MHA's Board of Directors. The DPO's duties include -

a. Informing and advising MHA and its Colleagues regarding the processing of data in accordance with Data Protection regulations and national law.

b. Ensuring the Information Governance policies, including Privacy Notices, align with Data Protection regulations or national law.

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

d. Maintaining a record of personal data held by MHA and processing activities.

e. Acting as a point of contact for and cooperating with the Information Commissioners Office (ICO) - the UK's Data Protection Authority.

f. Informing and updating the ICO regarding MHA's current or intended personal data processing activities as necessary.

g. The establishment and operation of a system for logging and providing prompt and appropriate responses to the rights of data subjects.

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

i. Informing MHA's senior directors and managers of any potential corporate, civil and criminal penalties which may be levied against MHA and/or its colleagues for violation of applicable Data Protection laws.

j. Data Protection compliance monitoring.

k. Ensuring the establishment of procedures and contractual provisions for obtaining compliance with this policy by any third party who –
   - provides personal data to MHA
   - receives personal data from MHA
   - has access to personal data collected or processed by MHA.

3.4 Compliance Monitoring

The Data Protection Officer will carry out a Data Protection Compliance audit for all locations and departments to determine the level of compliance. Each audit will, as a minimum, assess -

a. Compliance with Policy in relation to the protection of personal data, including –
   - Raising awareness.
   - Training of colleagues.

b. The effectiveness of Data Protection related operational practices, including –
   - Data subject rights (including involving the DPO).
   - Personal data transfers.
   - Personal data incident management.
   - Personal data complaints handling.
   - The level of understanding of Data Protection policies and Privacy Notices.
   - The accuracy of personal data being stored.
   - The conformity of Data Processor activities.
   - The adequacy of procedures for redressing poor compliance of personal data breaches.

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

3.5 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 shall 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.

3.6 Data Protection by Design

Data Protection by Design requires that all risks involving personal data are considered when –
- new systems are being considered and implemented.
- changes are being made to systems affecting the use of personal data.
- security or access criteria are being changed.
- business processes involving personal data are changed.

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 must engage with the Data Protection Officer or MHA's Change Team, as appropriate, who will carry out the DPIA. The subsequent findings of the DPIA must then be reviewed and approved. Where applicable, the IT Department, as part of its IT system and application design review process, will cooperate with the Data Protection Officer and MHA's Change Team to assess the impact of any new technology uses on the security of personal data.

4 DATA PROTECTION PRINCIPLES

MHA must apply the following GDPR principles to govern its collection, use, retention, transfer, disclosure and destruction of personal data:

Principle 1: Lawfulness, Fairness and Transparency
Personal data shall 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 or opt-in, (lawfulness).

Principle 2: Purpose Limitation
Personal data shall 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 shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

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

Principle 4: Accuracy
Personal data shall 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 shall 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 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 shall 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 shall 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.

5 DATA COLLECTION

5.1 Data Sources

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 (see **IG002b**) 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 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.

5.2 The Legal Basis for Data Use

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.

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 a need exists to request and receive the consent of an individual prior to the collection, use or disclosure of their personal data, MHA is committed to seeking such consent.

The Data Protection Officer, in cooperation with MHA's Change Team, and other relevant business representatives, shall establish a system for obtaining and documenting data subject consent for the collection, processing, and/or transfer of their personal data. The system must include provisions for -

- Determining what disclosures should be made to obtain valid consent.
- Ensuring the request for consent is presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.
- Ensuring the consent is freely given - i.e. is not based on a contract that is conditional to the processing of personal data that is unnecessary for the performance of that contract.
- Documenting the date, method and content of the disclosures made, as well as the validity, scope of the consents given.
- 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 their of personal data and the personal data is collected from the data subject all appropriate disclosures (see **IG002b**) will be made unless one of the following apply –

- The Data subject already has the information
- A legal exemption applies to the requirements for disclosure and/or Consent.

The disclosures may be given orally, electronically or in writing. If given verbally, the person taking the details must use form 'Data Protection Policy - Verbal Record Form' **(IG002c).** 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. Specifically that –

- A Privacy Notice covers the contract.
- The collected personal data will only be used to fulfil the contract.
- Only data necessary for the contract will be requested.
- There is a means for ensuring that the data is correct.
- MHA's Retention Schedule details the retention period.
- The data will be kept secure only accessed on a need to know basis.

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 Orders 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 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

On occasion MHA may use the legal basis of 'legitimate interest' in order to process personal data or to process personal data for a purpose different to the original intention. For example:

- MHA will share employee details with the Rewards Gateway. This is not required for employment but MHA considers the benefits provided to employees a legitimate interest. Colleagues are entitled to opt-out of this service.
- 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.

5.3 Privacy Notices

MHA will make available Privacy Notices covering the processing of personal data, e.g. for the following –

- Staff (contractors, employees & volunteers).
- Care home residents.
- Retirement living residents.
- Live at Home Members.
- Supporters (including donors and fundraisers).
- Property Sales.

Privacy Notices should be provided at the point that the data subject provide their data. Where possible notices should be provided using the same media as the data collection - i.e. any paper forms should reference the privacy notice directing them to the website and offer a phone number to request a copy by post. If the information is collected over the phone then information about the privacy notice should be given over the phone, pointing the person to the website or offer to send it by post.

All Privacy Notices must be approved by the Data Protection Officer prior to use.

5.4 Cookies

MHA will provide an online 'Cookie Notice' for each website made available by MHA fulfilling the requirements of applicable law.

All Cookie Notices must be approved by the Data Protection Officer prior to use or publication on an external website.

6 DATA USE

6.1 Data Processing

MHA uses personal data for the following purposes –

- The administration of MHA's responsibilities as an employer.
- The general running and business administration of MHA.
- To provide services to MHA's service users.
- The ongoing administration and management of customer services.
- MHA's supporter activities.

The use of personal information should always be considered from the data subject's perspective and whether the use will be within his / her expectations or if s/he is 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 then provide their details to third parties for marketing purposes.

MHA will process personal data in accordance with all applicable laws and applicable contractual obligations. More specifically, MHA will not process personal data unless at least one of the following requirements are met -

a. The data subject has given consent to the processing of their personal data for one or more specific purposes.

b. Processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract.

c. Processing is necessary for compliance with a legal obligation to which the Data Controller is subject.

d. Processing is necessary to protect the vital interests of the data subject or of another natural person.

e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller.

f. Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, where the data subject is a child).

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 Data Protection Officer before any such processing may commence.

In any circumstance where consent has not been gained for the specific processing in question, MHA will address the following additional conditions to determine the fairness and transparency of any processing beyond the original purpose for which the personal data was collected –

a. Any link between the purpose for which the personal data was collected and the reasons for intended further processing.

b. The context in which the personal data has been collected, regarding the relationship between data subject and the Data Controller.

c. The nature of the personal data, whether Special Categories of Data are being processed, or whether personal data related to criminal convictions and offences are being processed.

d. The possible consequences of the intended further processing for the data subject.

e. The existence of appropriate safeguards pertaining to further processing, which may include encryption (minimum encryption level AES-128), anonymisation or pseudonymisation (using codes, making anonymous, using alternative names)

6.2 Special Categories of Data

MHA will only process Special Categories of Data (also known as sensitive data) where the data subject expressly consents to such processing or where one of the following conditions apply –

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

b. The processing is necessary for the establishment, exercise or defence of legal claims.

c. The processing is specifically authorised or required by law.

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. Further conditions, including limitations, based upon national law related to the processing of genetic data, biometric data or data concerning health.

In any situation where Special Categories of Data are to be processed, prior approval must be obtained from the Data Protection Officer 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.

6.3 Children's Data

Children are unable to consent to the processing of 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.

Should MHA foresee a business need for obtaining parental consent, relating to processing personal data of a child, guidance and approval must be obtained from the Data Protection Officer. An example of where we would need to process consent is the use of photos or video footage where a child is included.

6.4 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 –
   - a law prohibits erasure.
   - erasure would impair legitimate interests of the data subject.
   - the data subject disputes that their personal data is correct and it cannot be clearly ascertained whether their information is correct or incorrect.

6.5 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.

6.6 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.

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.

6.7 CCTV

MHA uses CCTV system for crime prevention and detection. To comply with data protection law and the Information Commissioners 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' (not MHA) is the Data Controller
   - The system is used for crime detection and prevention
   - The contact telephone number is 01332 296200

d. the system must be password protected with need to know access.

e. monitors must be turned off when not being used.

f. the camera quality should be crisp so faces can be identified.

g. there must be 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. the recording should be restricted to a rolling 30 days.

7 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'. 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.

8 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'. A summary of the personal data related security measures is provided below –

a. Prevent unauthorised persons from gaining access to processing systems in which personal data is processed.

b. Prevent persons entitled to use a data processing system from accessing personal data beyond their needs and authorisations.

c. Ensure that personal data during electronic transmission cannot be read, copied, modified or removed without authorisation.

d. Ensure, where feasible, that access logs are in place to establish whether, and by whom, the personal data was accessed, modified on or removed from a data processing system.

e. Ensure that where processing is carried out by a data processor, the data can be processed only in accordance with the instructions of the Data Controller.

f. Ensure that personal data is protected against undesired destruction or loss.

g. Ensure that personal data collected for different purposes can and is processed separately.

h. Ensure that personal data is not kept longer than necessary.

9 DATA SUBJECT RIGHTS

The Data Protection Officer will establish a system to enable and facilitate the exercise of data subject rights –

1. **Right to be informed**
2. **Right of access**
3. **Right to rectification**
4. **Right to erasure**
5. **Right to restrict processing**
6. **Right to data portability**
7. **Right to object**
8. **Rights in relation to automated decision making and profiling.**

All requests for Right of Access (or Subject Access Request) must be directed to the Data Protection Officer. 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 completed response to each request must be provided within one calendar month of the receipt of the identity verification or the written request from the data subject, if no identity verification is required. If the request is made electronically the information shall be provided electronically unless otherwise requested.

If “Rights of Access” requests are repetitive, vexatious or excessive the request may be denied (see **CP102**, Unacceptable Behaviours Policy).

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

10 COMPLAINTS HANDLING

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

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

11 REPORTING OF POLICY BREACHES

All security incidents possibly involving personal data must be reported to the Data Protection Officer, by email (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).**

12 LAW ENFORCEMENT

In certain circumstances, it is permitted that personal data be shared **without** the knowledge or consent of a data subject. This is the case where the disclosure of personal data is necessary for any of the following purposes –

a. The prevention or detection of crime.
b. The apprehension or prosecution of offenders.
c. The assessment or collection of a tax or duty.
d. By the order of a court or by any rule of law.
e. To aid a Regulator to carry out their activities

If MHA receives a request for personal information from the Police or other law enforcement agency then the request must be made in writing to the Data Protection Officer, quoting the legal basis for the request. Most agencies have a specific form to be used which details the exemption covering the request. The form must quote the Data Protection Act (2018) Schedule 2 Part 1.2, not the Data Protection Act (1998) Section 29. It is important to note that even if a form is presented stating the reason for the request this does not necessarily mean the information has to be provided. MHA's Data Protection Officer must process all such requests. If a request is made in person or over the phone, colleagues must ask for an email or letter to be sent.

No information shall be provided to any agency unless it has been reviewed and redacted by the Data Protection Officer to protect other individuals identified in the documents.

The provided documents must be signed for, see **IG002d.**

13 REGULATORY EXEMPTIONS

CQC (and other Regulators – CIW, CIS) has power that grant them full access to records in MHA's services.

Under section 63(2)(b) of the *Health and Social Care Act 2008*, a person authorised to carry out an Inspection on behalf of CQC may access, inspect and take copies of any documents or records held by the service that they are inspecting, where they consider it 'necessary or expedient' to do so for the exercise of CQC's 'regulatory functions'.

In order to exercise these powers the representative should hold a duly authenticated document showing they have been granted these powers. This 'document' may be printed on rear of the inspector's CQC identity badge or a separate letter of document from CQC.

Anyone taking part in a CQC Inspection who does not hold such a document cannot and must not attempt to exercise CQC's powers to access medical and care records. However, they may be shown relevant medical and care records where there is a legitimate reason for doing so - e.g. in relation to an investigation.

14 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 for their employees.

The training and procedural guidance will consist of, at a minimum, the following elements –

a. The Data Protection Principles as in Section 4 above.
b. Each staff member's duty to use and permit the use of personal data only by authorised persons and for authorised purposes.
c. The use of procedures and forms adopted to implement this policy.

d. The correct use of passwords.

e. The importance of limiting access to personal data - e.g. locking the computers when leaving the desk, ensuring that individual elements of resident's data is only accessible to those who need to access it.

f. Securely storing manual files, print outs and electronic storage media - e.g. clean desk.

g. The procedures and safeguards for all transfers of personal data outside of the MHA's network and physical location.

h. Proper disposal of personal data by using secure shredding facilities.

i. Any special risks associated with departmental activities or duties.

15 DATA TRANSFERS

MHA may transfer personal data to internal departments or third-party recipients located in EU 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. A Data Protection Impact Assessment (DPIA) must be completed. 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.

MHA may only transfer personal data where one of the transfer scenarios listed below applies and the data subject has been made aware of the transfer –

a. The data subject has given consent to the proposed transfer.

b. The transfer is necessary for the performance of a contract with the data subject.

c. The transfer is necessary for the implementation of pre-contractual measures taken in response to the data subject's request.

d. The transfer is necessary for the conclusion or performance of a contract concluded with a third party in the interest of the data subject.

e. The transfer is necessary for the establishment in relation to legal claims.

f. The transfer is necessary to protect the vital interests of the data subject.

15.1 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 password-protection and encryption, where necessary).

15.2 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.

Where the third party is deemed to be a Data Controller, MHA will enter into, in cooperation with the Data Protection Officer, an appropriate agreement with the controller to clarify each party's responsibilities in respect of the personal data transferred.

Where the third party is deemed to be a Data Processor, MHA will enter into, in cooperation with the Data Protection Officer, an adequate processing agreement with the Data Processor. The agreement must require the Data Processor to protect the personal data from further disclosure and to only process personal data in compliance with MHA instructions. In addition, the agreement will require the Data Processor to implement appropriate technical and organisational measures to protect the personal data as well as procedures for providing notification of personal data breaches. MHA has an Information Sharing Policy (**IG009**) which colleagues must follow.

When MHA is outsourcing services to a third party (including Cloud Computing services), we will identify whether the third party will process personal data on its behalf and whether the outsourcing will entail any Third Country - i.e non-EU countries - transfers of personal data. In either case, working with the Data Protection Officer, we will make sure to include adequate provisions in the outsourcing agreement for such processing and Third Country transfers.

The Data Protection Officer must conduct regular audits of processing of personal data performed by third parties, especially in respect of technical and organisational measures they have in place. Any major deficiencies identified will be reported to and monitored by MHA's Leadership Team.

16 POLICY MAINTENANCE

All enquiries / queries about this policy, including requests for exceptions or changes must be directed to the Data Protection Officer DataProtectionOfficer@mha.org.uk.

17 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