

Data Protection Policy

IG02 Information Governance

August 2024

**Contents**

[1 Introduction 2](#_Toc175063715)

[2 Scope and Purpose 2](#_Toc175063716)

[3 Definitions 3](#_Toc175063717)

[4 Governance 4](#_Toc175063718)

[5 Data Protection Principles 5](#_Toc175063722)

[6 Data Subject Rights 10](#_Toc175063726)

[7 Reporting of Policy Breaches 11](#_Toc175063728)

[8 Data Protection Training 11](#_Toc175063729)

[9 Data Protection by Design and by Default 11](#_Toc175063730)

[10 Data Processing 12](#_Toc175063731)

[11 Sharing Personal Data 18](#_Toc175063738)

[12 Roles and Responsibilities 21](#_Toc175063742)

[13 Training and Monitoring 24](#_Toc175063743)

[14 Communication and Dissemination 24](#_Toc175063744)

[15 Guidance Notes 25](#_Toc175063745)

[16 Resources 28](#_Toc175063749)

[17 Version Control 29](#_Toc175063750)

1. Introduction
   1. Colleagues will be aware of, understand and know how to implement the Data Protection Act 2018 (DPA), the UK General Data Protection Regulation (UK GDPR) and the Privacy of Electronic Communications Regulation (PECR) when processing personal data.
2. Scope and Purpose
   1. All MHA colleagues and third-party organisations that process Personal Data for or on behalf of MHA, must:
   * Ensure that all colleagues are aware of their roles, responsibilities and accountability and fully comply with the Legislation as described in this and other Information Governance (IG) policies.
   * Create and maintain a level of awareness of the need for confidentiality and information security as an integral part of MHA’s day to day business.
   * Protect information assets under MHA’s control.
   1. An organisation that processes 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, reputational damage, and/or fines.
   2. MHA’s CEO and Executive Leadership Team (ELT) 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 may result in disciplinary action or business sanction.
   3. The Legislation does not relate to records of the deceased, please refer to Records of the Deceased Policy.
3. Definitions

| Term | Definition |
| --- | --- |
| **Colleagues** | A Data Subject who works part-time or full-time for MHA under a contract of employment (staff), volunteer agreement (volunteer) or as an independent contractor. |
| **Data Controller** | The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; |
| **Data Processor** | A natural or legal person, or third-party which processes personal data on behalf of the Data Controller. |
| **Data Protection Legislation,**  **Legislation** | This includes: the UK General Data Protection Regulations (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR) as updated from time to time. |
| **Data Subject** | An identifiable living person. For MHA this is past & present, living: colleagues, residents, family members and supporters or any person for whom MHA processed or has processed personal data |
| **Document**  **(see Record)** | A piece of writing that contains information, e.g. a recipe. |
| **IT Policy** | The IT policy (IT1 Computer Use Policy) and IT guidance, which may be updated from time to time. |
| **Legal Hold (or Litigation Hold)** | The need to ensure that documents, relevant to the subject matter of a pending or anticipated lawsuit, investigation, or inquiry, are kept safe from being edited, deleted, or destroyed. |
| **Personal Data** | Any information (including opinions and intentions) which relates to a Data Subject. |
| **Process, Processed, Processing** | Any operation or set of operations performed on Personal Data or on sets of Personal Data, by automated or manual means. Operations may include collect, record, organise, sort, store, edit, retrieve, use, disclose, combine, restrict, erasure, or destroy. |
| **Record**  **(see Document)** | A piece of writing that contains information that can be used as evidence, e.g. that a recipe was followed on a specific date, food temperatures were checked, food was served to x, y & z. |

1. Governance

Data Protection Officer

* + 1. As required by the Legislation, MHA has a Data Protection Officer (DPO). The DPO operates independently and is granted all necessary authority. The DPO reports to MHA’s Company Secretary who is a member of the ELT and has direct access to MHA’s Board of Directors. The DPO’s duties include:

1. Advising MHA and its Colleagues regarding the processing of data in accordance with the Legislation.
2. Providing guidance when a Data Protection Impact Assessments (DPIAs) are being completed.
3. Recording all incidents involving personal data and determining when the ICO and/or data subjects must be informed of a breach.
4. Data Protection compliance monitoring.
5. Ensuring the establishment of procedures and contractual provisions with third parties, as necessary.

Data Controller

* + 1. MHA is typically the Data Controller for 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).
    2. MHA may enter in contracts with third parties - e.g. local authorities, Clinical Commissioning Groups - to provide a service on their behalf. MHA and the third-party will typically be processing the personal data for different purposes, though the purpose may be related. The parties will normally 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.
    3. Any contract referring to MHA as a Joint Controller must be reviewed by the DPO before signing.

Data Processors

* + 1. MHA may engage with the external parties to carry out processing on behalf of MHA. These are Data Processors for MHA.
    2. MHA must have a contract with its Data Processors. All contracts with Data Processors must be reviewed by the DPO to ensure compliance with the Legislation.
    3. To comply with the UK GDPR, the data processor’s contract must comply with Article 28. MHA has a Data Processing Agreement template (IG02a) that can be used to facilitate this.

1. Data Protection Principles
   1. MHA must apply the following principles when processing personal data:

**Principle 1: Lawfulness, Fairness and Transparency.** MHA:

* + must have a lawful basis for processing personal data - e.g. contract, consent (opt-in) or Legitimate Interest (opt-out) (lawfulness)
  + must make it clear what data will be processed and how it will be processed, and
  + must inform the Data Subject how their personal data will be processed, through Privacy Notices and Cookie Policies.

**Principle 2: Purpose Limitation.** MHA must specify exactly what the personal data collected will be used for and only use for that purpose.

**Principle 3: Data Minimisation.** MHA must collect the minimum amount of data to carry out the required processing.

**Principle 4: Accuracy.** MHA must have in place procedures for identifying and correcting out-of-date, incorrect, and redundant personal data.

**Principle 5: Storage Limitation.** MHA must have a retention policy in place which specified how long personal data will be retained, before being deleted, destroyed, or anonymised (see IG01a).

**Principle 6: Integrity & Confidentiality.** MHA must use appropriate technical and organisational measures in place that ensures the integrity and confidentiality of the processed personal data.

**Principle 7: Accountability.** MHA must be able to demonstrate that the six principles are being applied through detailed policies, procedures, training, and regular audits.

The Lawful Basis for Processing Personal Data

* + 1. There are six lawful bases for the processing of personal data:

Consent from the Data Subject.

* + - 1. When replying on consent, MHA must request, receive, and record the consent before or at the point of collection, providing a copy of MHA’s Privacy Notice.
      2. The business stake holder must establish a system for recording the consent and provide a simple method for consent to be withdrawn at any time.
      3. Consent may be given verbally, electronically or in writing. If given verbally, the person taking the details must create a record of the consent, e.g. by using the Verbal Consent Record Form.
      4. Consent for activities in the care home or retirement living scheme, including the use of photos in “their home,” is captured on Consent Form (care homes) or Consent Form (Retirement Living/Day Care).
      5. Consent for photos, videos, and quotes for use on social media, websites and in printed materials must be recorded, e.g. using the Media Consent Forms .

Performance of a Contract

* + - 1. All contracts created by MHA or to be signed by MHA must be reviewed by MHA’s DPO, before signing.
      2. When a privately funded resident moves into a care home or retirement living scheme, they must sign a contract with MHA - Residential Care Agreement.
      3. Where MHA has a contract with the Local Authority or NHS to provide care for the resident, MHA will rely on Legitimate Interest to process the residents personal data. Contracts with local authorities and the NHS must recognise MHA as an independent Data Controller.

Legal and Statutory Requirement

* + - 1. MHA will comply with all legislation that requires the sharing of Personal Data.
      2. There is different legislation in the devolved countries regarding sharing personal data with healthcare professionals and social workers for the provision of care. The DPO will ensure the legislation is adhered to.

Protection of Vital Interests

* + - 1. In an emergency, MHA will share the necessary information to protect the life of data subjects. Where residents have a Do Not Resuscitate Order on file this will take precedence.

Tasks carried out for Public Interest

* + - 1. These will include, but are not limited to 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.

Legitimate Interest

* + - 1. To determine if Legitimate Interest can be relied upon a Legitimate Interest Assessment Form must be completed and returned to the DPO. 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.
      2. At public events MHA, my use Legitimate Interest as the lawful basis for taking and using photos or videos at the event. At such events, the event organiser must display, at all entry points and around the event, Event Photography Posters as found on the intranet.
      3. MHA will not use the legal basis of Legitimate Interest for processing photos of children under the age of eighteen or residents with dementia. A Media Consent Form (paper/digital) must be completed by the child’s parent/legal guardian or the resident’s Lasting Power of Attorney/Deputy.
      4. Where Legitimate Interest is the lawful basis for communications, the communication must explain the right to opt-out and include contact options, e.g. by including an email address or phone number.

Processing Special Categories of Data

* + 1. MHA will only process Special Categories of Data (also known as sensitive data) where one of the following conditions apply:

1. The data subject has provided consent, e.g. MHA Communities members, volunteers.
2. The processing is necessary regarding MHA’s obligations for employment.
3. The processing is necessary to protect the vital interests of the data subject or of another person who is physically or legally incapable of giving consent.
4. MHA will process the special category data of residents for, “the provision of health or social care.”
5. The processing is authorised or required by law or an exception under the Legislation.
   * 1. Prior to new processing of Special Category Personal Data, a DPIA must be completed and signed off by the DPO.
     2. Appropriate protection measures must be in place when Special Categories of Personal Data are processed.
     3. As required by the Data Protection Act 2018 (Schedule 1 Part 4) MHA must have in place, and keep updated, an Appropriate Policy Document, covering the processing of Special Category and Criminal Offence data.

Data Protection Annual Audit

* + 1. The DPO will carry out a Data Protection Annual Audit for all locations and departments to determine the level of compliance. Each audit will, as a minimum, assess:

1. Application of the Legislation’s principles
2. Staff awareness and training
3. Processing of Data Subject’s rights, including the involvement of the DPO
4. Incident and breach reporting to the DPO
   * 1. The Data Protection Annual Audit Form is an Excel spreadsheet which can accessible via the intranet Please be aware that the audit file changes each year, so each year the new audit file must be used. Do not edit last year’s audit file!
     2. The audit period is October to April each year.
     3. The audit must be completed and emailed to the DPO by the 30th of April.
     4. If 95% was not achieved, an action plan must be created and completed. A follow-up audit should be completed and submitted within 3 months.
     5. The ELT representative will be informed of any major deficiencies.
5. Data Subject Rights
   1. The DPO will be responsible for assisting data subjects in exercising their rights:
   * Right to be informed
   * Right of access
   * Right to rectification
   * Right to erasure
   * Right to restrict processing
   * Right to data portability
   * Right to object
   * Rights in relation to automated decision making and profiling.
   1. All requests for Right of Access (or Subject Access Request) must forwarded 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 must be sent within one calendar month of the date the request was received from the data subject, if no identity verification is needed, or within one calendar month of receipt of the proof of ID. If the request is received electronically the information will be provided electronically, unless otherwise requested.
   2. For more information see the Data Subject Rights Policy.

Complaints Handling

* + 1. 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.
    2. 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.

1. Reporting of Policy Breaches
   1. All security incidents involving personal data must be reported to the DPO, by email or phone the same day the incident is identified.
   2. For more information see the Information Incident Reporting Procedure.
2. Data Protection Training
   1. All MHA Colleagues that process personal data must have their responsibilities under this policy outlined to them as part of their induction training. In addition, MHA colleagues must complete their annual data protection training, currently the Confidentiality and Information Handling course.
3. Data Protection by Design and by Default
   1. Data Protection must be considered at the initiation phase of all new projects involving personal data. This is to include, but is not limited to:
   * Implementing new IT systems for storing or accessing personal data,
   * Implementing a change to an IT system or business process that involves personal data,
   * Developing procedures that involve personal data,
   * Projects where data is may be transferred outside the UK,
   * Data sharing initiatives, and
   * Using personal data for new purposes.
   1. All colleagues involved in projects involving personal data must engage with the DPO and must complete a Data Protection Impact Assessment **before** a project commences and **before** contracts are signed. They may also need to involve the Change Team or the IT Department.
   2. The DPIA ensures that privacy is considered at the design stage of projects and by default by those involved. Use of DPIAs can lead to:
   * Potential problems being identified at an early stage, with mitigation often being simpler and less costly.
   * Increased awareness of privacy and data protection concerns within the project.
   * Legal requirements being met from the outset leading to a reduced chance in any data protection breaches.
   * The project not being stalled at a later point due to unforeseen personal data risks.
   1. The DPIA must include a complete list of the personal data being processed for the project.
   2. The DPIA must be treated as a living document, which is reviewed and updated throughout the life cycle of the project, especially when:
   * Any of the responses to 1a or 1b change.
   * The personal data be processed and the uses of the personal data change.
   * IT systems change, e.g. if the IT system initially scoped in the DPIA changes.
   1. All DPIAs must be submitted to the DPO at the initiation of the project. The subsequent findings of the DPIA must then be reviewed and approved.

* 1. To comply with the GDPR’s principle of ‘lawfulness, fairness and transparency’ the data subjects need to be informed of how their data is processed. If the project is changing what data is processed, how the data is processed, the legal basis for the processing, the sharing of the data or the processing outside the UK then MHA’s Privacy Notices must be updated.

1. Data Processing

Data Collection

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

1. The nature of the business purpose necessitates collection of the personal data from other persons or bodies - e.g. contract with Local Authority or NHS.
2. 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.
3. 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:
4. One calendar month from the first collection or recording of the personal data.
5. At the time of first communication if used for communication with the data subject.
6. Prior to disclosure if it is to be disclosed to another recipient.

Using Personal Data

* + 1. MHA uses personal data for the following purposes:

1. The administration of MHA’s responsibilities as an employer.
2. The general running and business administration of MHA.
3. To provide services to people using MHA’s services.
4. The ongoing administration and management of customer services.
5. MHA’s supporter activities.
6. Direct marketing and fundraising
   * 1. 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 MHA will use their details to respond to a request for information about the products and services they have enquired about. However, it may not be within their reasonable expectations that MHA would use or share their details for marketing purposes.
     2. 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 “5.1 The Lawful Basis for Processing Personal Data.”
     3. There are 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 DPIA or LIA may be required.

Direct Marketing including Fundraising

* + 1. Direct marketing covers 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.
    2. Marketing also includes advertising the services that MHA offer, engaging with supporters to promote MHA and all aspects of fundraising.
    3. 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, and regarding website cookies.

Promoting MHA and Fundraising

* + - 1. 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.
      2. **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.
      3. Where a new use of personal data for marketing is being considered a Legitimate Interest Assessment form (IG02e) 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

* + - 1. The legal basis for market of property is consent. The consent will be recording in the Sales Department’s Customer Relationship Management (CRM) system.

Digital Marketing

* + - 1. 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.
      2. 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.
      3. 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.

Children’s Data

* + 1. Children, aged under eighteen, 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, there may be other lawful bases used, e.g. contract for employees under the age of eighteen.
    2. All proposed processing of children’s data 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.

Profiling & Automated Decision-Making

* + 1. Any proposed profiling or automated decision-making system or process, including the use of artificial intelligence, must have a signed of DPIA **before** testing or implementation.
    2. 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:

1. Object to the automated decision-making being carried out.
2. Obtain an explanation for the automated decision process.
3. Review the logic used by the automated system.
4. Provide additional or revised data.
5. Contest the automated decision.
6. Have a human carry out a review of the automated decision.

CCTV

* + 1. MHA uses CCTV system for crime prevention and detection. To comply with data protection law MHA has Data Protection Impact Assessments covering the use of CCTV (internal, external and ad-hoc internal) as CCTV systems are deemed to be a high risk to the rights and freedoms of individuals. If a CCTV is being considered, changes to coverage is being considered, a system is being replaced or removed the DPO must be consulted.
    2. The DPIA concludes that all CCTV systems must:

1. only use the system for crime prevention and detection - i.e. not watching staff unless it relates to a crime.
2. make sure the cameras only cover MHA property - i.e. not roads, paths, or property outside our boundaries.
3. 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.
4. be password protected with need-to-know access.
5. have monitors turned off when not being used.
6. record with a quality such that faces and vehicle registration numbers can be identified – day and night.
7. Ideally, 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. If the system cannot do this MHA must arrange for the process to be done by a third-party.
8. Have recording restricted to a rolling 30 days.
9. Have a document detailing:
   * The roles authorised to access it (e.g. Manager, deputy, admin, maintenance) – ensuring only these roles currently have access,
   * How the password is set and changed, and
   * How the system is used (including exporting footage/photos and blurring/deleting faces and registration numbers).
10. Sharing Personal Data
    1. Information sharing, in the context of this policy, means the disclosure of personal data between business areas within MHA or from MHA to one or more organisations. Information sharing can take the form of -
    * A reciprocal exchange of data,
    * One or more organisations providing data to a third-party or parties,
    * Multiple organisations pooling information and making it available to each other,
    * Multiple organisations pooling information and making it available to a third-party or parties, or
    * Exceptional, one-off disclosures of data in unexpected or emergency situations

Transfers between MHA Entities

* + 1. 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).

Transfers to Third Parties in the UK

* + 1. MHA will only permit the transfer of personal data to third parties when they are assured that the information will be processed legitimately and be protected appropriately by the recipient. Where third-party processing takes place, MHA will determine if the party is to be a Data Controller, or a Data Processor of the personal data being transferred.
    2. Personal information may be shared with other organisations, where necessary and proportionate: to assess needs, to ensure and review the provision of a quality service; for safeguarding; and to investigate complaints or potential legal claims.
    3. Before data sharing commences a DPIA should be completed and returned to the DPO.
    4. 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. The proposed contract must be reviewed by the DPO for compliance with the legislation.
    5. All decisions and reasoning related to the information sharing must be documented. In all circumstances of information sharing, colleagues must ensure that:

1. When information needs to be shared, sharing complies with the law, guidance, and best practice.
2. Only the minimum information necessary for the purpose will be shared.
3. Individuals’ rights will be respected.
4. Confidentiality must be adhered to unless there is a robust public interest or a legal justification in disclosure.
5. Reviews of information sharing must be conducted to make sure the information sharing is meeting the required objectives and is still fulfilling its obligations.
   * 1. Where Special Category Personal Information needs to be shared for non-care purposes the purposes for sharing need to be defined and limited, and additional requirements such as recorded informed consent may be required to enable lawful sharing.
     2. When personal information is shared, both the disclosing and receiving organisations must have procedures that meet the requirements of law and guidance and make clear to colleagues the appropriate working practices. In most circumstances these procedures (and the law and guidance on which they are based) should be set out in the Data Sharing Agreement.

Data Sharing Agreements

* + - 1. The Information Commissioner’s Office recommends Data Sharing Agreements between organisations sharing personal information (see IG02i, Data Sharing Agreement Template).
      2. Data Sharing Agreements set out rules to be adopted by the organisations involved in an information sharing operation. They may form part of a contract between organisations.

International Data Transfers

* 1. MHA may need transfer personal data to a recipient located outside the UK. The contract covering the transfer must detail the safeguards in place to protect the individuals’ personal data.
  2. Before the transfer occurs, MHA’s DPO must review the contract and assess the documented safeguards. These could include UK adequacy regulation, an International Data Transfer Agreement (IDTA) or Standard Contractual Clauses (SCCs).

1. Roles and Responsibilities

| Role | Responsibilities |
| --- | --- |
| **All Colleagues** | All colleagues must understand and apply to the Information Governance policies. |
| **Senior Managers** | Shall be individually responsible for the security of their physical environments where information is processed or stored. They are responsible for:  Ensuring that their team are aware of the information security policies, procedures, and user obligations applicable to their area of work.  Determining the level of access to be granted to specific individuals.  Ensuring colleagues have appropriate training for the systems they are using.  Ensuring that any data breaches are reported to the Data Protection Officer. |
| **Information Asset Owners (IAO)** | * An information asset is any piece or collection of information stored by MHA and processed as a single unit - e.g. colleagues personal file, resident’s care record. It is something we can’t replace without cost, time, skill, and resources. * All service managers (CH, RL & MHA Communities) are IAOs. All department heads are IAO. IAOs are responsible and accountable for the security and processing of all their information assets, they will: * Lead and foster a culture that values, protects, and uses the information assets lawfully. * Know who has access to the assets, and why, ensuring use is monitored and compliant with policy. * Understand and address risks to the asset and provide assurance to the SIRO. * Ensure there is a lawful basis for processing and for any disclosures. * Maintain adequate records the assets that are processed. |
| **Head of Talent Acquisition and Shared Services** | * The Head of Talent Acquisition and Shared Services is responsible for ensuring that the contracts of all colleagues (permanent and temporary) are compliant with the requirements of information governance and that data protection is included in inductions. |
| **Associate Director of IT** | * Develop IT policies that implement best business practice, ensuring they are applied throughout the business. * Ensure effective management and security of MHA’s IT infrastructure and equipment. * Responsible for and being the point of contact for IT security within MHA. * Monitoring potential and actual security breaches, informing the DPO as appropriate. * Develop and implement an IT Disaster Recovery Plan. |
| **Caldicott Guardian** | The Senior Nurse Advisor is the Caldicott Guardian for MHA. The Caldicott Guardian will:   * Work alongside the DPO to make sure that the personal information about people who use MHAs services is used legally, ethically, and appropriately and that confidentiality is maintained in relation to the storage, management and sharing of this information. * Provide leadership and informed guidance on complex matters involving confidentiality and information sharing regarding personal information for MHA’s residents. * Play a key role in ensuring that MHA satisfies the highest practical standards for handling the person information of people receiving care and support from MHA. * Apply the eight Caldicott Guardian Principles * Act as the conscience of MHA, providing impartial and independent advice. * Represent and champion information governance requirements and issues at senior management team and board level where appropriate, being and integral part of the overall information governance framework. * Play a key role in advising and ensuring that the Caldicott Principles are applied in digital and paperless systems. |
| **Data Protection Officer (DPO)** | MHA will ensure that there is always one person with overall responsibility for data protection, the DPO.  The DPO will:   * Implement policies and procedures to embed the data protection principles and the rights of Data Subjects. * Ensure data protection training is provided to all colleagues and provide additional guidance and support as required or requested. * Keep records as required by the data protection legislation. * Risk assess each breach/incident and log with the ICO, as necessary. * Inform the Board of breaches or incidents that are reportable to the ICO. |
| **Senior Information Risk Owner (SIRO)** | The General Counsel / Company Secretary is responsible for information risk within MHA and advises the Board on the effectiveness of information risk management across the Organisation. The SIRO will -   * Implement and lead MHA’s Information Governance Risk Assessment and Management processes. * Advise the Board on the effectiveness of information risk management across MHA. * Receive training as necessary to ensure s/he remains effective in the role as SIRO. |
| **Chief Executive Officer (CEO)** | * Overall responsibility for strategic and operational management, including ensuring that MHA’s policies comply with all legal, statutory, and good practice guidance requirements. |

1. Training and Monitoring
   1. All colleagues must complete the following within three months of commencement of employment and annually thereafter, achieving a “pass” grade:
   * Confidentiality and Information Handling, and
   * Cyber Security Awareness
2. Communication and Dissemination
   1. This policy is disseminated and implemented within all MHA services through MHA’s channels of communication.
   2. Each colleague’s line manager must ensure that all teams are aware of their roles, responsibilities.
   3. This policy will be available to the people we support and their representatives in alternate formats, as required.
   4. Queries and issues relating to this policy should be referred to the Standards and Policy Team [policies@mha.org.uk](mailto:policies@mha.org.uk).
3. Guidance Notes

Anonymisation and Pseudonymisation

* + 1. When personal data is being used for secondary purposes, e.g. exports for analysis or reporting, consideration should be taken on whether the individual needs to be identifiable or whether the identifiers can be removed with the aim still being achieved.
    2. There are two ways of removing the identifiable data:
  + **Anonymisation**. This involved removing all identifiable data. E.g. an extract that contained:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| StaffNo | first name | surname | DOB | Address | Religion | Role | Salary |

Would become:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | DOB | City | Religion | Role | Salary |

This level of anonymisation is irreversible and does not allow multiple sets of data to be linked together.

* + **Pseudonymisation**. This removes the identifiable data as above but adds a reference which would mean the process could be reversed by the person that holds the key, i.e. StaffNo=RefNo, and would allow multiple sets of data to be linked together using the reference. E.g the above example may become:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| RefNo |  |  | DOB | City | Religion | Role | Salary |

This would allow other records to be linked to the reference. E.g. training records with the same RefNo will relate to that staff member:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RefNo |  |  | Training Course | Score | Date |

Who should carry out the anonymisation?

* + - 1. There are typically three sets of people involved in a process that may require anonymisation:
  + The Data Owner
  + The export requester/analyser
  + The recipient of the final data
    - 1. Where possible the Data Owner should carry out whichever level of anonymisation is deemed appropriate, preferring full anonymisation over pseudonymisation. If this is not possible the DPIA needs to consider if it is acceptable for the requester to have access to the full data.
      2. All data export processes require a DPIA detailing considerations for anonymisation.

Completing the Data Protection Annual Audit

* + 1. The audit is an Excel spreadsheet which can be found on the intranet (IG02g). Please be aware that the audit file changes each year, so each year a new audit file must be started. Do not use last year’s audit file!
    2. The audit must be completed between October and April each year.
    3. The audit is broken down into sections. Each section has multiple questions, which required a: “Yes”, “No”, or in some cases an “[other]” response.
    4. Some questions required additional information, identified by a grey box under the Yes, No response. Please place the additional information in this box, not the comment box. The grey boxes are used by the scoring system, the comment boxes are not.
    5. Please respond to all questions, ensuring no lines still have “Select” as the answer. Note any lines that have the “**\*\***” error marking, which means it needs completing or is non-compliant.
    6. The responsibility for submitting the audit varies across MHA:
  + **Central Support:** The ELT director must ensure the audit is completed for each department in their area. They may delegate completion of the audit.
  + **Care Homes:** The home manager is to self-assess their home. They may delegate completion of the audit to the Administration Manager but must check and affirm the audit. Random checks may then be carried out.
  + **Retirement Living & MHA Communities:** The area manager is to assess their schemes.

Completing the DPIA

* + 1. The DPIA form (IG02h) contains all stages of the assessment:
  + Stage 1a & 1b Initial Assessment
  + Stage 2 Data Identification and Processing
  + Stage 3 Consultation Process
  + Stage 4 Assess necessity and proportionality
  + Stage 5 Risks and Mitigations
  + Stage 6 Risk after mitigations implemented
  + Stage 7 Sign off and record of outcomes
    1. The areas to be completed are dependent on the outcome of Stage 1a & 1b.
    2. All required stages must be completed in order and must be completed prior to submission to the Data Protection Officer for review.

1. **“Processing Summary” and “What processing is involved?”**

All projects and changes require the completion of these sections of the DPIA form. If “Yes” is the answer to any of the types of processing the complete form must be completed.

1. **Data Identification and Processing**

During this section you will provide details about the processing of personal data for the proposed works.

Please provide as much information as possible, providing additional documents as appropriate, e.g. contracts, supplier documentation.

1. **Consultation Process**

Identify who needs to be involved. Determine if external Data Processors need to be consulted. Determine if the Data Protection Officer and the IT Director need to be involved at this stage.

1. **Assess necessity and proportionality**

The section looks at the legal basis for the work and helps to determine if the amount of processing justifies the required outcomes.

1. **Risks and mitigations**

Identify the risks and mitigations at the initiation stage and any residual risks after the mitigations are applied.

1. **Sign off and record of outcomes**

The final stage requires sign off by the DPO: for measures to be added to the project plan, for residual risks and by the Data Protection Officer and those consulted.

1. Resources
   1. MHA policy documents, procedures, and guidance:
   * Data Processing Agreement Template
   * Verbal Consent Record Form
   * Media Consent Form (paper)
   * Media Consent Form (digital)
   * Legitimate Interest Assessment Form
   * Appropriate Policy Document
   * Data Protection Annual Audit
   * Data Protection Impact Assessment form
   * Data Sharing Agreement Template
2. Version Control

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Version Date | Revision Description / Summary of Changes | Author | Next Review Date |
| 4 | July 2024 | Review and merging of IG002, IG005, IG009 & IG011 and appendices | Data Protection Officer | July 2027 |
| 5 | August 2024 | 10.6.2 references changed to DPIA, ICO Code of Practice which no longer exists. | Data Protection Officer | July 2027 |