Data Protection Policy

1. DEFINITION

1.1. As a landlord and employer, MHA holds a wide range of data on the business and its properties, personal information on a variety of people, including customers (current, former and prospective), Board Members, current and former employees, job applicants, contractors and suppliers. This information is used for example to allocate its properties, manage customers' tenancies, recruit, manage and pay its employees, and monitor its performance and customer feedback. This information is held in a range of physical and computerised forms.

1.2. MHA is committed to protecting the rights of individuals' privacy with regard to the processing of personal data and any information we hold about them. We demonstrate this through operating within the requirements of the Data Protection Act 2018 and UK General Data Protection Regulations (UK GDPR) ("**Data Protection Law**") with regards to collecting, storing, processing, divulging, sharing and disposing of personal information that relates to a living individual who can be identified. MHA is a controller and processor of personal data **("Data Controller")**. MHA is registered as a Data Controller with the Information Commissioner's Office and we take privacy and the security of personal information very seriously.

- **Data Controller** means organisations that process personal data. Manningham Housing Association Ltd and Firebird Homes Ltd are data controllers.
- **Data Protection Law** means the UK GDPR and the Data Protection Act 2018 (DPA 2018)
- **Personal data** means data which relates to any living individual who can be identified: from this data; or from that data and other information that is in the possession of, or is likely to come into the possession of the data controller. It includes, for example, name, date of birth, images and photographs whether we hold it on paper or electronically
- **Data subject** means a person who we hold information about
- **Special Categories of Personal Data** is data about an individual's racial or ethnic origin, political opinions, sexual orientation, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings - any use of sensitive personal data should be strictly controlled in accordance with this policy. Its important to understand and note that where we wish to process special category data or criminal conviction data, we will also need to identify a lawful basis to rely on under Article 6 of the UK GDPR. Following that an additional condition will then need to be relied on under Article 9 for special category data and Article 10(1) for criminal conviction data

1.3. **Business purposes**

The purposes for which personal data may be used by us:

- Housing management, HR, administrative, financial, regulatory, legal, payroll and business development purposes

Business purposes include the following:

- processing information about our tenants in paper and/or electronic form. As well as general contact, tenancy and financial information this will include sensitive personal data

- we may also share relevant and limited tenant data with building contractors and customer survey agencies. In both cases, we are still responsible for the safe keeping and privacy of tenant data
- Compliance with our legal, regulatory and corporate governance obligations and good practice
- Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests
- Ensuring business policies are adhered to (such as policies covering email and internet use)
- Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information
- Investigating complaints
- Recruiting, inducting, training and managing MHA employees and Board Members
- Ensuring safe working practices, monitoring and managing employee access to systems and facilities and employee absences, administration and assessments
- Monitoring employee conduct, disciplinary matters
- Marketing our business
- Improving services
- Statistical research

2. BACKGROUND AND CONTEXT

2.1. The data protection principles under UK GDPR (Article 5) relate to the processing of personal data (UK GDPR) and state that:

Lawfulness, fairness and transparency	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject
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
Data minimisation	Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
Accuracy	Personal data shall be accurate and, where necessary, kept up to date
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 are processed
Integrity and 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, using appropriate technical or organisational measures
Accountability	The controller shall be responsible for, and be able to demonstrate compliance with UK GDPR

2.2. The Principles require that personal information:

2.2.1 Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met. The conditions for processing are set out in the Data Protection Law. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

a. The individual whom the personal data is about has consented to the processing

b. The processing is necessary:

   i. in relation to a contract which the individual has entered into; or

   ii. because the individual has asked for something to be done so they can enter into a contract

c. The processing is necessary because of a legal obligation that applies to us (except an obligation imposed by a contract)

d. The processing is necessary to protect the individual's "vital interests". This condition only applies in cases of life or death, such as where an individual's medical history is disclosed to a hospital's A&E department treating them after a serious road accident

e. The processing is necessary for administering justice, or for exercising statutory, governmental, or other public functions

f. The processing is in accordance with the new "legitimate interests" condition defined in UK GDPR

2.2.2 Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes

2.2.3 Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed

2.2.4 Shall be accurate and where necessary, kept up to date

2.2.5 Shall not be kept for longer than is necessary for that purpose or those purposes

2.2.6 Shall be processed in accordance with the rights of data subjects under the Act

2.2.7 Shall be kept secure i.e. protected by an appropriate degree of security

2.2.8 Shall not be transferred to a country or territory outside the UK, unless that country or territory ensures an adequate level of data protection

2.3. MHA and all employees who process any personal information about other people will ensure that it complies with this Data Protection Policy.

3. AIM

3.1 The aim of this policy is to ensure that:

- Employees, Board Members, volunteers and contractors have clarity about maintaining confidentiality and understand the circumstances for disclosure of information
- we protect the people we hold personal information about
- we process personal and sensitive data in line with the Data Protection Act ~~1998~~ 2018 and UK GDPR
- we follow good practice

- we protect ourselves from the impact of a breach of our legal and regulatory responsibilities

3.2 This policy sets out how we seek to protect personal data and ensure that all MHA employees and Board Members understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires employees to ensure that the Data Privacy Manager (DPM) is consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

3.3 The content of this policy is applicable to all staff, volunteers and Board members regardless of their role at MHA.

4. WHEN WILL THIS POLICY BE ACTIVATED?

4.1. The policy covers the processing of personal data whose use is controlled by Manningham Housing Association (MHA). MHA is registered with the Information Commissioner's Office (ICO) for the purposes of processing personal data under the Data Protection Act: Manningham Housing Association Ltd **Registration Number: Z728485X**

4.2. It applies to all employees, contractors and consultants who process data on behalf of the organisation. Personal and sensitive data applies to both computer and manual records. Any breach of the Act or failure to follow this Data Protection Policy may, depending on the circumstances, result in performance and/or disciplinary proceedings or legal action.

4.3. We will communicate this policy to all employees, Board Members, volunteers, service partners and consultants and explain their responsibilities under this policy.

4.4. We will ensure that our service partners contract contains information regarding data protection and retention or we will ask our service providers to sign a Data Sharing Agreement and assess any risks to MHA around data processing done on our behalf via our Service Partner Due Diligence Questionnaire. Regular monitoring of these arrangements will be carried out dependent on the scale and length of the contract and the data processing carried out.

5. KEY PRINCIPLES

5.1. MHA is committed to working according to the principles as set-out in the Act (see section 2 above), and will apply these in the following areas:

- Responsibilities (Section 6)
- Privacy Notices – Transparency of Data Protection (Section 7)
- Data Security (Section 8)
- Use of Information Technology (Section 9)
- Mobile Working (Section 10)

- Employee Records (Section 11)
- Rights of Data Subjects (Section 12)
- Rights to Access Information (Section 13)
- Right to be Forgotten (Section 14)
- Disclosure of Data (Section 15)
- Data Privacy Impact Assessments (Section 16)
- Data Audits and Data Registers (Section 17)
- Retention and Disposal of Data (Section 18)

5.2. The Data Protection Law applies to everyone working for us, including Service Partners and volunteers (Manningham Customer Panel, Complaints Learning Forum). We will follow the principles of the Act when we deal with personal information:

- We will say what we are going to do with personal information before we collect it (unless it is obvious). Our forms and other methods of collecting personal information will contain a clear explanation of what we will do with the information and who we might share it with
- Where consent is identified by us at the appropriate lawful processing ground we will always take steps to ensure that requires affirmative action on the part of the consent giver. This means that silence, pre-ticked boxes or inactivity will not be sufficient to indicate consent. We will also take steps to ensure that data subjects are easily able to withdraw their consent to processing at any time and that any withdrawal of consent must be promptly honoured.
- We will only use personal information for the purpose we collected it. If we want to use personal information for different or incompatible purposes from that disclosed when it was first obtained, we will inform the data subject of the new purposes beforehand and where necessary obtain their consent
- The personal information we collect and hold will be relevant and fit for purpose. We will not collect or record irrelevant or excessive information
- We will make sure the personal information we hold is accurate and up to date
- We will only keep information for as long as we need it and destroy it securely when it is no longer useful to us
- We will uphold the rights of the people we hold information about:
    - If someone wants to see or have a copy of their personal information, we will deal with their request promptly (please refer to section 13 for further detail) (unless the DPM has confirmed that the Data Protection Law permits an extension of this time period)
    - If a person feels that their information is inaccurate, we will consider this carefully and correct our records following MHA Right to Rectify procedure
    - If a person asks that we no longer use their information because it is causing them harm or distress, we will follow MHA Right to Erasure procedure
- We will keep information secure at all times. We will make sure there are appropriate technical and organisational measures in place to prevent information being lost, stolen or seen by people who aren't authorised to see it.

- We will not pass information to countries outside the UK, unless a specific project requires us to do so, in which case we will notify you and in all cases only where the UK has issued regulations confirming that the country to which we transfer the personal data ensures an adequate level of protection for the data subject's rights and freedoms or alternatively, failing that where appropriate safeguards are in place or where the data subject has provided explicit consent to the proposed transfer after being informed of any potential risks

6. RESPONSIBILITIES

6.1. The organisation is the 'data controller' under the Act.

All employees, volunteers and Board Members are expected to read and to comply with our data protection policy and procedures.

All those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within the organisation.

Advice and guidance will be provided by the Data Privacy Manager.

We will take all reasonable steps to ensure that:

- all employees who handle personal information as part of their job are appropriately trained and supervised
- all employees understand their responsibilities for following good data protection practice
- all employees avoid, recording personal opinions not based on fact about a Data Subject. These comments will be disclosable
- personal information is not disclosed either accidently or deliberately either verbally or in writing to any unauthorised person or organisation

Employees who have responsibility for supervising apprentices, interns, students or volunteers involved in work which requires the processing of personal data are required to ensure that they are fully aware of the Data Protection Principles and the requirements of this Policy, and the need to obtain the consent of any data subjects involved as appropriate.

6.2. **The Data Privacy Manager (DPM)**

The person with day to day control of data protection compliance is the Data Privacy Manager (DPM). They are responsible for owning and operating a framework for assessing risks to the information we hold and for investigating incidents following a breach or potential breach of information security.

The Data Privacy Manager is specifically responsible for:

- Keeping the Executive Team updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as customers and employees who wish to know the data that is being held on them
- Checking and approving third party contracts or agreement regarding data processing when necessary

The Data Privacy Manager is responsible for co-ordinating subject access requests (where a person asks to see or have a copy of the personal information we hold about them). They will make sure requests are dealt with quickly and always within 30 days from receiving the request in writing and being able to confirm the identification of the requester (unless they have decided that the Data Protection Law permits an extension of this time period in any particular case). Refer to section 13.

6.3. The Corporate Project Manager is responsible for electronic information security. They will make sure that appropriate technical measures are in place to protect the personal information that we hold electronically.

7. PRIVACY NOTICES – TRANSPARENCY OF DATA PROTECTION

7.1 Being transparent and providing accessible information to individuals about how we will use their personal data is important for MHA.

In many situations MHA obtains personal data as part of a simple transaction, however, in other situations further personal and special category personal information may be required, in these cases our privacy notices (which are available to read on our website) inform individuals about what we do with personal data. The term ‘privacy notice’ is used to describe all the privacy information that we make available or provide to individuals when we collect information about them.

The following are details we will generally provide in privacy notices:

- What information is being collected
- Who is collecting it
- How is it collected
- Why is it being collected
- How will it be used
- Who will it be shared with
- Identity and contact details of any data controllers
- Retention period

7.2 MHA implements a call recording service which is activated on certain MHA staff landlines. Customers are notified that the call may be recorded and why before the conversation is opened. This notice to customers is executed through a pre-recorded message in the telephone welcome recording before connection is made to any staff.

7.3 MHA staff will on occasion record meetings via audio/visual recordings on the Microsoft Teams platform. If a recording take place, it is the responsibility of the individual that actions the recording to inform meeting attendees and ask for permission off all attendees before the recording starts. The recordings will not be kept any longer than necessary and in the case of Board or Committee meetings, the recordings will be saved securely (which access to digital files being protected where necessary) and deleted once the formal minutes of a meeting are approved.

8. DATA SECURITY

8.1. All users of personal information provided by MHA are responsible for ensuring that any personal information that they hold about other people:

a) Is kept securely in terms of physical security of offices and filing cabinets with the level of security appropriate to the level of confidentiality and sensitivity of the material

b) For paper records, this means being kept in a lockable room with controlled access, or kept in a locked drawer or filing cabinet. For electronic records, this means ensuring online folders are only accessible by authorised staff or are filed on designated electronic filing systems

c) Is not disclosed in any form to any unauthorised third party

d) Printed data should be disposed of in the confidential waste disposal unit when it is no longer needed

e) Data stored on a computer should be protected by strong passwords that are changed regularly

f) Data stored on memory sticks provided by the Corporate Project Manager or DPM, must be locked away securely when they are not being used

g) The DPM must approve any cloud used to store data

h) Data should be regularly backed up in line with the company's backup procedures

i) Data should never be saved directly on to the hard drive of mobile devices such as laptops, tablets or smartphones

j) All servers containing sensitive data will be protected by security software and industry leading firewall and virus protection.

8.2. Wilful unauthorised disclosure will usually be a disciplinary matter and may be considered gross misconduct or could potentially lead to legal proceedings.

8.3. Should a member of staff be subject to a disciplinary or engage in vexatious conduct towards the organisation, it is MHA's right to monitor their working habits and behaviour to ensure they are not wilfully causing a breach or handling personal data irresponsibly.

9. USE OF INFORMATION TECHNOLOGY

9.1. Employees must never divulge their username or password to anyone, and never write it down or store it insecurely. If you do have to make a record of your log in details ensure these are kept somewhere secure.

9.2. All laptops will be assessed for risks of data security. Those deemed to be at significant risk will have full boot-up disk encryption.

9.3. All other electronic devices such as handheld devices, iPads and mobile smartphones must be password protected. No sensitive personal data must be saved on such devices.

9.4. Care should be taken to ensure that desktop PCs and laptop screens are not visible except to authorised employees and that passwords are kept confidential. Logged In PCs/laptops should not be left unattended without logging out.

9.5. Employees are not permitted to send attachments containing the personal details of customers or colleagues to external email addresses, unless we have a formal data sharing arrangement with the recipient organisation. This includes a prohibition on sending personal details to employees' own personal email accounts.

9.6. Employees and managers assessed to need them will have memory sticks issued to them. Any other employees who need to use a memory stick for work purposes should agree this with their manager and collect one from the Corporate Project Manager or DPM.
No personal memory sticks should be used for business purposes for any reason. If an external visitor brings information on a memory stick, employees should ensure that the device is first scanned for viruses before being used.

9.7. The Corporate Project Manager will inform the IT support contractor immediately of any leavers. Accounts will then be disabled immediately.

9.8. When a person is signed off sick by a doctor, it may be necessary to enter the email account to put an 'out of office' message on and divert and archive emails. This task must be completed by the Corporate Project Manager.

9.9. As stated in 8.3, MHA has the right to monitor the ICT activity of any employee who continues to use MHA equipment, following a disciplinary, vexatious episode or if they leave the association.

10. MOBILE WORKING

10.1 When working away from the office employees should:

a) Ensure that when they are working on documents containing personal information covered by the Act that they are mindful of data security as they are when they are working in the office.

b) Work exclusively on the server/network and do not save any MHA documents on personal computers or laptops, on desktops, or on personal memory sticks

c) Ensure data is transferred at the next reasonable opportunity onto the server or network and deleted from the device, where the server/network is not available and where information is saved to the hard drive

d) Do not take hard copies of information out of the office that are not needed

e) Consider carefully how hard copies of confidential information is disposed of. If necessary, please retain until you can return to the office, and dispose of it using MHA secure bins.

f) Consider how you store your laptop and documents when you are not using them. Do not leave any items in your car.

10.2 MHA provides mobile phones for some members of staff, laptops are issued to all members of staff which enables employees to monitor emails if they wish to do so whilst they are mobile working.

10.3 MHA does not authorise MHA 365 email accounts to be activated on personal mobile devises. If a personal or sensitive data breach occurs that is traceable to a personal device, the owner of the personal device would be held accountable and could be held liable for the breach alongside MHA.

11. EMPLOYEES RECORDS

11.1. Employees are responsible for:

- Ensuring that any personal data supplied to MHA is accurate and up-to-date
- Changing any personal information such as change of address, next of kin details, medical notes etc. on the Cascade HR system

11.2. Managers should not hold personal details of employees unless these are securely locked away. Employees who want to access their own information, or managers who wish to access that of their employees, should contact the MHA HR Assistant.

11.3. An employee who considers this Data Protection Policy has not been followed in respect of personal data about himself/herself should first raise the matter with their line manager, who will in turn raise the issue with the Data Privacy Manager.

12. RIGHTS OF DATA SUBJECTS

12.1 All data subjects are entitled to:

- Know what information MHA holds and processes about them and why
- Gain access to it their personal data
- Keep their data up to date
- Request the organisation to rectify, block, erase or destroy inaccurate information
- Prevent processing likely to cause unwarranted damage or distress
- Prevent processing for the purposes of direct marketing
- Seek compensation where it is alleged that they have suffered damage, or damage and distress, because of a breach of the Data Protection Law

13. RIGHTS TO ACCESS INFORMATION (SUBJECT ACCESS REQUESTS)

13.1. Individuals (Data Subjects) have the right to access / request to see the data held about them both in electronic and paper files. This is known as a Subject Access Request (SAR).

13.2. All employees will be made aware of how to recognise and respond to a SAR although this will be fully co-ordinated by the Data Privacy Manager.

13.3. For customers wanting access to their information, a verbal or written SAR can be accepted, however if a verbal request is made the DPM will encourage a written request so that there are no discrepancies about what has been requested.

13.4. In most cases the data subject must receive access to information one month from the first date of receipt of a request and after we have received the necessary information to satisfy ourselves to the identity of the person making the request.

13.5. Where we process a large quantity of information about an individual, the Act permits us to ask the individual to specify the information the request relates to. The UK GDPR does not introduce an exemption for requests that relate to large amounts of data, but we may be able to consider whether the request is manifestly unfounded or excessive, and act accordingly.

13.6. Employees wanting access to their HR file should request this through the MHA HR Assistant.

14. RIGHT TO BE FORGOTTEN

14.1 A data subject may request that any information held on them by MHA is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies.

On receiving a request by a data subject to delete or remove information held about them, the DPM will make an assessment following the Right to Erasure procedure (if necessary in conjunction with the Executive Team) about the request and if it should be fulfilled. Any exemptions and legal requirements will be considered before making the decision.

15. DISCLOSURE OF DATA

15.1. We will carry out security checks before discussing or disclosing personal information to a customer to make sure we are dealing with the correct person.

15.2. We will make sure that personal data is not disclosed to different departments within MHA, to Board Members or to volunteers acting on behalf of MHA (Manningham's Customer Panel, Complaints Learning Forum etc.) unless there is a legitimate reason for having this information and it is covered under section 2.1.1 point's a-f.

15.3. MHA will ensure that personal data is not disclosed to unauthorised third parties who include family members, friends, service partners, external organisations and partner agencies. All employees should exercise caution when asked to disclose personal data held on another individual to a third party. If in doubt seek help and clarification from your line manager or the Data Privacy Manager. We will make sure we have a person's permission before we give their personal information to anyone who wishes to act on their behalf (for example, a family member, solicitor or MP).

15.4. We will share information with third parties if we are required to do so by law, or if they have a court order. We may share information with other organisations if we are satisfied that:

- there is a valid reason to do so and;
- the law allows us to

15.5. When we give personal information to our suppliers and service partners to process on our behalf, we will make sure:

- there are adequate security arrangements in place to keep the information secure
- there is a suitable agreement (Data Sharing Agreement / Protocol) or contract in place that clearly outlines their responsibilities for managing the personal information they have been given
- that we do not provide excess personal information over and above the personal information that is relevant to the nature of the task or service in question

15.6. This policy determines that personal data may be legitimately disclosed where one of the following conditions apply:

- the individual has freely given express consent (e.g. a customer/member of employees has consented to MHA corresponding with a named third party)
- to pursue our legitimate interests (or those of a third party) for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects. where the disclosure is in our legitimate interests (e.g. disclosure to employees - personal information can be

disclosed to other employees if it is clear that those employees require the information to enable them to perform their jobs)

- where the organisation is legally obliged to disclose the data

15.7. Service Partners will be required to comply with MHA's Data Protection Policy in the disposal of their duties.

15.8. There may be circumstances when it is appropriate for MHA to share personal information with other organisations, for example if it relates to a criminal investigation. In any such circumstances further guidance should be sought from the Data Privacy Manager.

16. DATA PROTECTION IMPACT ASSESSMENTS

16.1 Data Protection Impact Assessments (DPIA's) are executed by project leaders before MHA starts a major project involving the use of personal or special category data; major refers to, processing data on a large and frequent scale or processing data which could be considered high risk to the rights and freedoms of individuals.

16.2 The DPM will be responsible for reviewing all Data Privacy Impact Assessments and ensuring that mitigations are in place to reduce risks identified. No high-risk activities will be implemented without the appropriate approvals.

16.2 When relevant, and when it does not have a negative impact on the data subject, privacy decisions and any technical IT settings will be set to the most private by default.

17. DATA AUDITS AND DATA REGISTERS

17.1 Regular data audits to manage and mitigate risks will inform MHA's data registers. The Registers contains information on what data is held, what the legal reasons for processing that data are, where it is stored, how it is used, where and when it is disclosed / shared, who is responsible and any further regulations or retention timescales that may be relevant.

18. RETENTION AND DISPOSAL OF DATA

18.1. The Act forbids the retention of personal data for longer than it is required. Once customers are no longer tenants / leaseholders of MHA, or once employees have left employment, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others and we will carry out periodic audits to ensure that we are complying with the principles and best practice.

MHA will follow the guidance as set out in the most recent National Housing Federation Document Retention Schedule.

18.2. Appropriate security measures are in place for the deletion or disposal of personal data. Personal data will be disposed of in a way that protects the rights and privacy of data subjects (e.g., shredding, disposal as confidential waste, secure electronic deletion).

18.3. Responsibility for establishing disposal mechanisms for documents in their areas of the business lies with the appropriate Manager and/or Director.

19. REPORTING DATA BREACHES

19.1. All employees have an obligation to report actual or potential data protection compliance failures to their manager or the DPM. This allows MHA to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures

19.2. UK GDPR contains an obligation on data controllers to notify supervisory authorities (the Information Commissioner's Office – ICO) of personal data breaches. In some cases this extends to the data subjects as well.

Article 4 of the Regulation defines a personal data breach:

> *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

If MHA becomes aware that a personal data breach has occurred it will without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO.

There is no need to do this where MHA can demonstrate that the breach is unlikely to result in a risk for the rights and freedoms of individuals. For example, a very minor data breach involving innocuous information about a few individuals.

Where the 72-hour deadline cannot be achieved, an explanation of the reasons for the delay should accompany the notification.

It is the responsibility of the DPM to seek appropriate advice and ensure that, where necessary, the ICO is notified about any relevant data breaches.

20. CUSTOMER IMPACT

20.1 All customers, as data subjects, are protected by this Policy. They will be provided with reassurance that their privacy is being protected and have clear procedures for requesting access to their information. Access to services covered under this policy will be fair and equitable for all. Any complaints regarding data protection and/or processing will be dealt with under the relevant complaints policy for customers or HR policy for MHA employees.

21. MONITORING AND REVIEW

21.1 The Data Privacy Manager is responsible for the monitoring and review of this policy on an ongoing basis, or when change in the law necessitates an immediate review.

A full and comprehensive review will be carried out by July 2026.

22. TRAINING

22.1 All employees including temporary employees will be made aware of this policy as part of their induction. Where employees are temporary the local manager is to ensure that these employees comply with the policy.

Employees training on data protection will be provided through the Data Privacy Manager, including on-line e-learning modules and skills based workshops and there will be an annual refresher for all employees reminding them of their responsibilities under this policy.

23. OTHER RELEVANT DOCUMENTS

23.1. This policy should be read in conjunction with the following relevant documents:

- Subject Access Request Procedure
- Privacy Notice(s)
- Cookies Notice
- All other data handling procedures

23.2. Main contact for further information: Data Privacy Manager.

Policy	Data Protection Policy
Policy No.	ARC08
Equality Impact Assessment Completed	Yes
Date approved by the Committee	Oct 2023
Date approved by the Board	November 2023
Next Review date	July 2026
Lead Officer	Executive Assistant/Data Privacy Manager