MHA Group
Data Protection Policy

Monmouthshire Housing
Tai Sir Fynwy

Great People, Great Homes, Great Location

Date: April 2016
Reviewer: Mared Dafydd

Date of Renewal	Considered last	Date uploaded to Inhouse	Author	Summary of changes
April 2019	April 2016		Mared Dafydd	New Policy
Department: Resources – Risk and Business Assurance				

Data Protection Policy

1. Introduction

1.1 As a Housing Association, MHA must collect, store and process data about its tenants, leaseholders and other customers to enable us to effectively manage our tenancies and deliver our services.

1.2 We may also collect personal data and sensitive personal data which will enable us to better understand our customers and tailor services to meet our customers' needs.

1.3 We will always aim to do this

- in the most effective and secure way
- lawfully
- fairly
- and by being honest and transparent with our customers

2. Purpose of the Policy

2.1 The purpose of this policy is to outline MHA's approach, policies and procedures in relation to collecting, storing and processing personal and sensitive information about our customers.

3. Definitions

3.1 Data – A record or information which is held electronically, on a computer (including e-mails) or in certain based filing system. Even if the record or information does not yet form part of a filing system, it's still considered as data.

3.2 Personal Data – Data (as defined above) which relates to an individual that can be identified from that data. This includes any expression of opinion about an individual. Types of personal data includes name, address, contact details, HR records,

3.3 Sensitive Personal Data – Personal data about an individual relating to:

- The racial or ethnic origin of an individual
- Their political opinions
- Their religious beliefs or other beliefs of a similar nature
- Whether they are a member of a trade union
- Their physical or mental health or condition
- Their sex life
- Their commission or alleged commission of any offence
- Any proceedings for any offence committed or they are alleged to have committed, the disposal of such proceedings or the sentence of any court in such proceedings

3.4 Record – Recorded information maintained as evidence of business activities and transactions eg application forms, tenancy agreements, Rent Statements, Letters, PDRs, supervision minutes.

3.5 ICO – Information Commissioner's Office - The ICO is the UK's independent body set up to uphold information rights.

3.6 Customer - For the purpose of this policy this will include, tenants, leaseholders, staff or any other individual we hold personal information about.

4. Approach

4.1 MHA will comply with the Data Protection Act 1998 (until the forthcoming EU Data Protection Reforms come into effect in 2018 – at that time, this policy will be amended).

4.2 MHA will collect and use personal data in accordance with the 8 principles of the Data Protection Act. These state that personal data must be:

- Processes fairly and lawfully
- Processed only for one or more specified and lawful purposes
- Adequate, relevant and not excessive in relation to the purpose
- Accurate, and where necessary, kept up to date
- Kept for no longer than is necessary for that purpose
- Processed in accordance with the rights of 'data subjects'
- Secure
- Not transferred outside of the European Economic Area without adequate level of protection

4.3 MHA will register annually with the ICO.

4.4 MHA will have established data protection policies and procedures which will be communicated effectively to staff and customers. All our services and practices will be carried out in accordance with these policies and procedures.

4.5 MHA will adopt a privacy by design approach which means that we will consider privacy and data protection implications at the start of projects or initiatives that involve the processing of personal data.

4.6 MHA will ensure Privacy Impact Assessments (PIA) are undertaken during the development, testing and delivery stages of any project and ensure staff are trained on carrying out these assessment

4.7 There will be defined data protection roles and responsibilities within MHA and training and support will be provided to ensure individuals understand their role and responsibility.

4.8 MHA will regularly carry out checks and tests to ensure we are complying with the policies and procedures.

5. Roles and Responsibilities

5.1 Board

5.1.1 The Board will seek assurance that MHA has effective policies and procedures in place to ensure it is complying with legislation with regard to Data Protection

5.1.2 It will seek assurance that Data Protection risks are being identified and managed effectively.

5.2 SMT

5.2.1 SMT will set the culture of the organisation in relation to Data Protection.

5.2.2 They will ensure that adequate policies and procedures are being produced and implemented to enable the effective management of personal data.

5.2.3 They will ensure that data protection risks are identified and managed.

5.2.4 They will ensure checks and tests are being carried out on compliance with policies and procedures.

5.3 Risk and Business Assurance Manager

5.3.1 The Risk and Business Assurance Manager will act as the Data Protection Lead within MHA

5.3.2 The role includes:

- Writing policies and procedures in relation to Data Protection – ensuring they are in line with legislation and good practice
- Ensuring policies and procedures are effectively communicated with staff
- Supporting managers and staff to ensure personal data is managed effectively and in line with policies and procedures
- Arranging Audits and Checks across the organisation
- Ensuring MHA are aware of current legislation and any changes to these legislations
- Investigate data protection breaches and report to the relevant body if necessary
- Lead on the coordinating responses to Subject Access Requests

5.4 IT Manager

5.4.1 The IT manager is responsible for implementing measures to ensure the security of personal data and records and carry out periodic and ad-hoc checks to test the effectiveness of the security measures.

5.5 Heads of Service, Managers and Staff

5.5.1 All staff have a responsibility to comply with the data protection policies and policies and procedures.

5.5.2 They should take all necessary steps to keep customers' personal data safe when working in the office or off-site.

5.5.4 They should report any breach that they are made aware of and escalate any data protection risks that are identified.

5.5.6 Staff should not discuss personal data or business sensitive information for non-work purposes.

6. Processing Data Fairly and Lawfully

6.1 MHA will have legitimate grounds for collecting and using personal data and will not use data in ways that have unjustified adverse effects on our customers.

6.2 MHA will be open and honest with customers and communicate clearly on what personal data is collected and to what purpose.

6.3 MHA will only collect and use personal data for the purpose we have specified. We will not use the data for any other purpose without our customers being informed.

6.4 MHA will have clear privacy statements in place which will ensure our customers know how the information about them will be used. These will be easily accessible on our website and will appear on all relevant documents and forms.

7. Data and Records Management

7.1 MHA will ensure that we have measures in place to ensure that the personal data we hold is accurate, adequate, relevant and not excessive to the purpose we have specified.

7.2 Measures will be in place to check that newly collected personal data is accurate, adequate, relevant and not excessive to the purpose we have specified.

7.3 Periodic weeding exercises will take place to remove inaccurate, inadequate, irrelevant data and data that is excessive to the purpose we have specified.

7.4 MHA will record have a record of the personal data sets and records we hold.

7.5 Records and personal data sets will have documented retention periods and a process will be in place to discard, delete or anonymise personal data or records as soon as they become surplus to requirements. This will ensure that data and record are not held for longer than is necessary.

7.6 When paper or electronic records are created MHA will put measures in place to ensure that:

- There is legitimate purpose for creating the record
- The record is titled and indexed for ease of disposal
- Confidential records are identified and appropriate security measures put in place

7.7 MHA will track the movement of records which are taken off-site to ensure their security.

7.8 MHA will identify and document the personal data and records that are essential to the continued functioning of the organisation. MHA's Business Continuity Plan will document how these records will be retrieved in the event of a major incident.

8. Security

8.1 MHA will have an established information security policy which will document the risks to the personal data we hold, security arrangements for access to personal data and records and periodic checks for compliance with policy.

8.2 Paper and electronic personal data and records will be stored securely with appropriate controls and higher levels of security around sensitive personal data. The controls will be appropriate to the nature of the personal data and the level of associated risk. Controls will include:

- Paper records will be stored in lockable offices or cabinets
- Access to data and records will be restricted on a role basis
- Strong passwords will be set for both network and system access
- Regular password changes will be enforced

8.3 System users' activities will be monitored to detect any abnormal use.

8.4 Periodic checks will be carried out to test the effectiveness of the security controls.

8.5 MHA will have established entry controls for offices and access will be restricted to specific areas within the building.

8.6 MHA will have a clear desk policy

8.7 MHA will have a secure printing system which require staff to manually release a printing job at the printer.

8.8 MHA will have a mobile working policy which documents the security risks of working off-site and the security measures put in place to protect data and records. Staff will be made aware of their responsibilities when working remotely.

9. Information Sharing

9.1 It will sometimes be necessary for MHA to share personal data with third parties. The third parties may include:

- Contractors carrying work out on our behalf
- The Police
- The Fire Service
- Organisations MHA are working in partnership with on a specific project
- The DWP

9.2 Before a decision is made to share personal data with a third party, MHA will consider:

- What is the sharing meant to achieve
- What information needs to be shared
- Who requires access to the shared personal data
- When should it be shared
- How should it be shared
- How can we check the sharing is achieving its objectives
- What risk does the sharing pose
- Could anything be achieved without sharing the data
- Does the ICO need to be informed of the sharing

9.3 Where required MHA will make data subjects aware of an intention to share data with a third party either through privacy statements, clauses in agreements or by asking for explicit consent for the data to be shared.

9.4 MHA understands that it still may be responsible for the personal data it shares, therefore before MHA shares information with a third party they will:

- Consider if sharing the personal data is lawful and what effect it will have on the data subject / subjects
- Ensure the third party provides sufficient guarantees about how they will protect the personal data; and
- Put enforceable contracts in place setting out information security conditions.

9.5 MHA will maintain a log of all decisions to share information.

9.6 Where information is shared with a third party on a regular basis, it may be necessary to have data sharing agreements. These agreements will be regularly reviewed.

9.7 MHA will have appropriate security measures to protect personal data in transit.

10. Subject Access Requests and Individual's rights

10.1 MHA will respect the rights of our customers to:

- Object to processing information about them that is likely to cause damage or distress
- Prevent processing for direct marketing
- Object to decisions being taken by automated means
- Have inaccurate personal data rectified, blocked erased or destroyed
- Claim compensation for damages caused by a breach of the Act

And respond accordingly.

10.2 MHA acknowledges that our customers has a right to gain access to the information MHA holds about them. We will respond to Subject Access in accordance with the ICO's guidelines and put a process in place to ensure requests are dealt with as effectively as possible and within 40 days.

11. Data Breaches and Incident Management

11.1 MHA will have a process in place for investigating data breaches

11.2 All breaches will be logged and if necessary, reported to the appropriate body.

11.3 MHA will ensure that lessons are learnt from any data breach and measures put in place to avoid a similar breach in future.

12. Training and Communication

12.1 Data Protection will be core training for all staff.

12.2 Training on specific areas will be delivered to staff on a role basis.

12.3 There will be a Data Protection Page on In-House which will include all relevant documentation and guidance notes.