

## **PRIVACY AND DATA PROTECTION POLICY**

### **1 Policy Statement**

The work of HAMA involves handling personal and sensitive data on identifiable individuals. This policy is to ensure that HAMA complies with the legal requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 with regard to the handling of such data, including responding to requests for copies of such data.

The policy applies to HAMA trustees and all workers at HAMA, paid or unpaid.

This policy should be read in conjunction with the separate Privacy Notice and Confidentiality Policy.

### **2 Responsibilities**

The trustees have overall responsibility for the implementation of this policy.

The Centre Manager is responsible for ensuring all workers are trained on this policy and is responsible for ensuring that the day-to-day management systems comply with this policy.

### **3 Personal Data Held**

Personal data is held on trustees and workers at HAMA to ensure, where appropriate, they meet the requirements of the Charity Commission, and they are suitable to work with vulnerable groups in accordance with the Safeguarding Vulnerable Groups Act 2006 and the Protection of Freedoms Act 2012.

Because of the nature of the advice service provided, personal data held on clients of HAMA includes financial information (e.g. income, expenditure, benefits, debts). Other information may also be held (e.g. medical information) provided it is relevant to the client's situation, and with their explicit consent.

### **4 Handling of the Data**

Data will be handled in accordance with the Privacy Notice and the Confidentiality Policy.

Data on suitability to work with vulnerable groups and data on clients are considered particularly sensitive and will be stored securely at all times: paper copies will be kept in a locked filing cabinet; electronic copies will be password protected. Access to the cabinets and the passwords will be restricted to those authorised by the Centre Manager or the trustees. Passwords will not be divulged to unauthorised people and will be changed periodically to ensure security.

### **5 Requests for Data Access (See Privacy Notice)**

Individuals may request a copy of data held on them by HAMA. The date the request is made will be recorded and all requests will be forwarded without delay to the Centre Manager (or in his or her absence to the Chair of Trustees or another trustee). The Centre Manager will review the request.



The requestor will be asked to provide sufficient evidence to confirm his or her identity. Once satisfied on the identity of the requestor, the Centre Manager will arrange for compilation of the relevant information. The Centre Manager will review the information prior to it being provided to the requestor to ensure it is appropriate and that it does not breach another person's right to confidentiality.

If the Centre Manager decides the information requested cannot be provided to the requestor, the requestor will be informed with, if appropriate, reasons for the refusal to provide the information.

The information requested, or response that the request cannot be fulfilled in time, will be provided within 1 calendar month of the request.

HAMA reserves the right to charge for requests, however under normal circumstances no charge will be made. If a charge is to be made, the requestor will be informed and asked to confirm that he or she still wishes to make the request.

## **6 Back-up of Data**

Data held electronically in SharePoint is constantly being backed-up to the Cloud and copies synced with all connected devices. A separate archive process stores copies of data so that they can be recovered if deleted accidentally from the live files.

All paper copies of documents, whether related to clients or to HAMA itself, will be scanned and stored electronically. Paper copies may be retained for immediate use, but can be destroyed if not needed.

## **7 Retention of Data**

See Appendix 1 of the Privacy Notice for a full table of retention periods for different documents.

Personal data on trustees and workers will be kept for six years following cessation of the person's work as a trustee or worker.

Personal data on clients may be kept for six years after the date of last contact with the client.

## **8 Revision History**

Originally approved by Trustees: 5 September 2013

Revision 1: Incorporation of data backup. Approved by Trustees: 12 June 2018

Revision 2: Approved by Trustees 11 June 2021

Revision 3: Approved by Trustees 25 June 2024

Next review June 2027