APPROPRIATE POLICY DOCUMENT

1. INTRODUCTION

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require an APD in place. (See Schedule 1 paragraphs 1(1) (b) and 5).

This document demonstrates that MHA's processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it outlines our retention policies with respect to this data. (See Schedule 1 Part 4).

1.1 Special category data

Special category data is defined in Article 9 of the GDPR as personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identifying a natural person
- Data concerning health or
- Data concerning a natural person's sex life or sexual orientation

1.2 Criminal conviction data

Article 10 of the GDPR covers processing in relation to criminal convictions and offences or related security measures. In addition, section 11(2) of the DPA 2018 specifically confirms that this includes personal data relating to the alleged commission of offences or proceedings for an offence committed or alleged to have been committed, including sentencing. This is collectively referred to as 'criminal offence data'.

Description of data processed
A brief description of each category of SC and CO data processed by MHA.

MHA processes special category data for:

a. **Staff (including applicants):** We process the special category data about our employees that is necessary to fulfil our obligations as an employer. Applicants provide equal opportunity information. This is not retained for unsuccessful applicants. It is used to create summary reports. Each staff member also completes a medical questionnaire to help MHA determine if special requirements need to be made regarding health or disabilities. Health information is also retained for statutory requirements regarding fitness to return to work after absence due to sickness.

b. **Care home and retirement living residents:** Residents using our services receive nursing of social care services - in order to provide these services we process medical and care information. As these are Regulated services, the data may be shared with the Regulator – CQC, CIW, CIS.

c. **Live at Home members:** Live at home members often go on day trips, etc. For their safety and wellbeing they consent to provide details regarding medical conditions and / or medication they are taking. This is deleted after the event.

d. **Fundraisers:** When fundraisers engage in an activity that requires a medical check (e.g. parachute jump, half marathon) the fundraiser will be asked to complete a medical questionnaire. This will be deleted after the event.

We also maintain a records of our processing as required by the GDPR Article 30, which is recorded in the Data Protection log: Information Asset Register and Process Log pages.

MHA's Privacy Notices, which include retention information, can be found on our website at www.mha.org.uk/PrivacyPolicy

Cont next page:

Schedule 1 condition for processing
The name and paragraph number of your relevant Schedule 1 conditions for processing.
Schedule 1 condition 2 does not need to be included in the Appropriate Policy Document but is mentioned for completeness. **Special Category Data** MHA applies the following DPA Schedule 1 conditions to: a. Staff (employees & volunteers, incl. applicants): 1. employment, social security and social protection (staff) 6. Statutory and government purposes (staff) 8. Equality of opportunity or treatment (applicants) 9. Racial and ethnic diversity at senior levels (applicants) b. Care Home and Retirement Living Residents: 2. health or social care 6. Statutory and government purposes 12. Regulatory requirements c. Live at Home members: 2. health or social care 6. Statutory and government purposes 8. Equality of opportunity or treatment d. Fundraisers: 2. health or social care **Criminal Offence Data** MHA applies the following DPA Schedule 1 conditions to: a. Staff (employees & volunteers, incl. applicants) 1. employment, social security and social protection

Cont next page

Procedures for ensuring compliance with the principles

The points below briefly explain how MHA processes SC and CO data in compliance with the principles of the GDPR.

Accountability principle

- MHA has appointed a Data Protection Officer, registered with the ICO, in compliance with the GDPR and DPA 2018.

- MHA's Data Protection Advisory Group meets quarterly with concerns or issues being passed to Executive Leadership Team. A report is provided to the Quality Board every quarter.

- Evidence of compliance is retained in the Data Protection logs which include:

a. Information Asset Register
b. Process Log
c. Subjects' Right's Log
d. Incident & Breach Log
e. Data Protection Impact Assessment Log
f. Legitimate Interest Log
g. Records of decisions

- We have a collection of Information Governance policies which include:

a. IG002 – Data Protection Policy
b. IG003 – Data Subject Rights
c. IG004 – Incident Reporting
d. IG005 – Privacy by Design, incorporating the DPIA
e. IG009 – Information Sharing
f. IG010 – Archiving
g. IG011 – Data Protection Quality Assurance, incorporating monthly checks and annual audit

- We put in place appropriate technical and organisational measures to protect the data:

a. Building entry control systems
b. Locks on doors and cabinets containing personal data
c. Complex password requirements for network access
d. Polices in place covering making email communication secure
e. Antivirus, malware and web filtering system
f. Audit system to monitor file access and email communications

Procedures for ensuring compliance with the principles cont:

The points below briefly explain how MHA processes SC and CO data in compliance with the principles of the GDPR.

Principle (a): lawfulness, fairness and transparency

- We have identified the lawful basis for our processing which is recording in the Data Protection Log in the Information Asset Register and Process Log pages. The lawful basis is generally: contract for staff, contract for residents and consent for: Live at Home members, sales enquires and for fundraising and marketing.
- We provide clear and transparent information about the data we process through our Privacy Notices. These are available for each type of data subject for whom we process data.
- We only process data as the data subject would expect.

Principle (b): purpose limitation

- We will not process personal data for purposes incompatible with the original purpose it was collected for, unless we have specific consent to process the data for an alternate purpose.
- If we are sharing data with another controller, we will document that they are authorised by law to process the data for their purpose.

Principle (c): data minimisation

- We collect personal data necessary for the relevant purposes and ensure it is not excessive. The information we process is necessary for and proportionate to our purposes. Where personal data is provided to us or obtained by us, but is not relevant to our stated purposes, we will erase it.

Principle (d): accuracy

- Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay.
- If we need to keep a record of a mistake, we clearly identify it as a mistake.

Principle (e): storage limitation

- All special category data processed by us for the purpose of employment or for the provision of a care service is set out in our retention schedule (IG001a).
- We determine the retention period for this data based on our: legal obligations, the necessity of its retention for our business needs and as required for our NHS contracts.
- Our retention schedule is reviewed regularly and updated when necessary.

Procedures for ensuring compliance with the principles cont:

The points below briefly explain how MHA processes SC and CO data in compliance with the principles of the GDPR.

Principle (f): integrity and confidentiality (security)

- We have put in place appropriate policies and technical and organisational measures to protect electronic and hard copy information.
- Electronic information is processed within our secure network.
- Hard copy information is processed in line with our security procedures.
- Our electronic systems and physical storage have appropriate access controls applied.
- A Data Protection Impact Assessment is carried out for all changes to business process or IT systems and for new IT systems.

Retention and erasure policies

Our retention and erasure practices are set out in our retention schedule (IG001a).

Special Category Data retained for:

a. Staff (employees & volunteers)	6 years after leaving
b. Care Home Residents	8 years after leaving or death
c. Retirement Living Residents	8 years after leaving or death
d. Live at Home members	1 year after cancelling membership

Criminal Offence Data retained for:

a. Staff (employees & volunteers)	6 years after leaving

Hard copy data is either shredded or destroyed under a secure data destruction contract.

IT equipment, potentially containing SC or CO data, is destroyed by a certified WEEE compliant recycler under contract.