AL-MAHDI INSTITUTE

Data Management and Cybersecurity Policy

1. INTRODUCTION

This policy outlines Al-Mahdi Institute's commitment to managing and protecting its data assets in a legal, secure, and efficient manner. It encompasses all forms of data, including electronic, paper-based, personal, and non-personal data.

2. PURPOSE

To ensure that data is:

- Collected and used fairly and lawfully.
- Stored safely and securely.
- Not disclosed unlawfully or inappropriately.

3. SCOPE

This policy applies to all employees, volunteers, contractors, and anyone else working on behalf of Al-Mahdi Institute.

4. DATA COLLECTION AND USE

- Data will only be collected for specific and legitimate purposes and will not be used in a manner that is incompatible with those purposes.
- Individuals will be informed about the data being collected about them and the intended use.

5. DATA STORAGE

- Data will be stored securely, ensuring protection against unauthorized access, loss, or damage.
- Electronic data will be stored on secure servers with appropriate access controls.
- Physical data will be stored in locked cabinets or rooms.

6. DATA SHARING AND DISCLOSURE

- Data will only be shared with authorized individuals or organizations and only when necessary.
- Any sharing of personal data will comply with data protection laws.

7. CYBERSECURITY

- All electronic data storage systems will be protected by up-to-date security software and firewalls.
- Employees will be required to use strong, unique passwords which are changed regularly.
- Regular backups of electronic data will be conducted.
- Employees will be trained on recognizing and avoiding phishing attempts, malicious software, and other cybersecurity threats.
- Any suspected data breaches will be reported immediately to the designated Data Protection Officer.

8. DATA RETENTION

- Data will not be kept longer than necessary.

- The Institute will establish and adhere to a data retention schedule, ensuring data is securely deleted or destroyed when no longer required.

9. RIGHTS OF INDIVIDUALS

- Individuals have the right to access data held about them and can request this from the Institute.
- Individuals have the right to request corrections to inaccurate data or deletion of their data in certain circumstances.

10. RESPONSIBILITIES

- All staff are responsible for ensuring they collect and use data in line with this policy.
- The Data Protection Officer is responsible for ensuring compliance with data protection laws, dealing with data access requests, and managing any data breaches.

11. REVIEW

This policy will be reviewed annually or in response to changes in relevant legislation.

Policy approved by the Board of Trustees on: 01/01/2023

Policy due for review: 01/01/2024