Policy name:	Data Protection Policy
Author:	Ben Butcher, Head of Operations
Approved by:	FAR Committee
Approved date:	21/10/24
Review date:	21/10/25

Revision number	Date	Details of Change(s)
1	21/10/24	

Contact information:

For questions, concerns or complaints regarding this Data Protection Policy or Magic Me's data protection practices, please contact:

Ben Butcher, Data Protection Officer
Address:
Magic Me,

Pott Street,
London,
E2 0EF
Email: info@magicme.co.uk
Phone: 02032226064

You can also complain to the ICO if you are unhappy with how we have used your data.The ICO's contact details are as follows:

Address:
Information Commissioner's Office,
Wycliffe House ,
Water Lane,
Wilmslow,
Cheshire,
SK9 5AF
Helpline number: 0303 123 1113
ICO website: https://www.ico.org.uk

Purpose:

Magic Me is committed to protecting the privacy and security of personal data in accordance with the UK Data Protection Act 2018 and the General Data Protection Regulation (GDPR). This Data Protection Policy outlines our approach to ensuring compliance with data protection legislation and safeguarding the personal data of our stakeholders, including but not limited to partners, volunteers, donors, beneficiaries, and employees.

Key documents:

- Live documents:
  - Magic Me Data Protection Register (contains full list of data held by the organisation including reasons for collection and storage)
  - Magic Me Data Maps (see separate key for colour coding)
  - Data Impact Assessments Folder (containing impact assessments on a project/function basis)
  - Data breach response process
- Templates:
  - Data Impact Assessment (DIA)
- Other relevant policies:
  - Privacy Notice (for website)
  - Cookie Policy (for website)
- Useful links:

- Information Commissioner's Office (ICO) support for organisations

Values:

Magic Me is a values based organisation. **As an organisation we work collaboratively, inclusively, creatively and thoughtfully.** When enacting the Data Protection Policy on a day-to-day basis it may be helpful for colleagues to consider that ensuring good data protection practice involves:

- Being thoughtful in the capture, storing and processing of personal data;
- Collaborating closely with all stakeholders to ensure they are aware of their data protection obligations and Magic Me policies;
- Being creative about ways to reduce the quantity of data we hold and how long we hold it for;
- Ensuring our inclusive practices and the sensitive personal data that underpins them is protected through robust implementation of our policies.

EDI & Anti-racism:

At Magic Me, we are committed to fostering an inclusive, diverse, and anti-racist environment, with particular sensitivity to data related to race and ethnicity. Wherever possible, we will anonymise or pseudonymise sensitive personal data to protect individual privacy and minimise risks. We only collect this data when necessary for legitimate purposes, such as monitoring inclusivity or meeting reporting obligations, and always in compliance with the UK Data Protection Act 2018 and GDPR.

When collecting sensitive data, we are transparent about its purpose and obtain explicit consent where required. Access to such data is strictly limited, and robust security measures are in place to ensure its protection. Magic Me is dedicated to using this data responsibly to promote fairness, equality, and respect for all individuals.

Scope:

This policy applies to all personal data collected, processed, and stored by Magic Me, whether in electronic or physical format. A list of the data collected by the organisation can be found on the Data Register and how it is processed can be seen via the data maps.It applies to all employees, volunteers, contractors (including artists), and third parties who handle personal data on behalf of Magic Me.

All Magic Me staff, volunteers and contractors are responsible for ensuring robust data protection practice. Magic Me's Data Protection Officer (DPO) is the Head of Operations (currently Ben Butcher) who can be contacted via dpo@magicme.co.uk.

Policy dissemination, implementation and execution

In order to ensure the efficacy of data protection practice, Magic Me commits to the following means of disseminating, implementing and executing the policy:

- Use of simple language and clear steps throughout the policy and supporting documents.
- Providing clear incident response plans that can be followed in the event of a data breach.
- Ease of access to the policy and other key data protection documentation.
- Annual data protection training including scenarios that could arise in Magic Me's context.
    - Training for new staff joining part way through the year.
- Data protection as a standing item at the weekly meeting to ensure colleagues keep its importance. To include bitesize training and questions to ensure practical understanding.
- Annual audits of data protection practice completed by the DPO.
- Annual data protection review with archiving and deletion of systems data.

Summary:

Principles of data protection: Magic Me adheres to principles such as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality, and accountability in processing personal data.

Data collection and processing: Personal data is collected and processed lawfully, with consent, as necessary for contractual obligations, legal obligations, vital interests, or legitimate interests. This includes activities like programme delivery, fundraising, marketing, and operational tasks.

Data retention: Personal data is retained for 6 years from the end of the relevant financial year unless otherwise specified in Data Impact Assessments. Individual projects or functions may have specific retention periods documented in these assessments.

Data subject rights: Magic Me respects data subjects' rights, including access, rectification, erasure, restriction of processing, data portability, objection to processing, and the right to file grievances with a regulatory body.

Data security: Appropriate technical and organisational measures are implemented to ensure the security of personal data against unauthorised processing, loss, destruction, or damage. This includes measures like two-factor authentication and ongoing staff training.

Data sharing and transfers: Personal data is only shared with third parties when necessary, with appropriate safeguards in place. International transfers comply with applicable data protection legislation.

Data breach management: Procedures are in place to assess and mitigate data breaches, including notifying the ICO and affected individuals within 72 hours of becoming aware of a breach.

Principles of data protection:

Magic Me adheres to the following principles of data protection:

- Lawfulness, fairness, and transparency: Personal data is processed lawfully, fairly, and transparently, with clear information provided to data subjects about the purposes of processing.
- Purpose limitation: Personal data is collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes.
- Data minimisation: Only personal data necessary for the intended purposes is collected and processed.
- Accuracy: Reasonable steps are taken to ensure that personal data is accurate and kept up to date.
- Storage limitation: Personal data is retained only for as long as necessary to fulfil the purposes for which it was collected.
- Integrity and confidentiality: Appropriate security measures are in place to protect personal data against unauthorised or unlawful processing and accidental loss, destruction, or damage.
- Accountability: Magic Me is responsible for demonstrating compliance with data protection principles and ensuring that appropriate measures are in place to fulfil its data protection obligations.

Key tenets of good data protection practice:

For any personal data held by Magic Me, it should be possible for anyone involved in processing the information to answer the following questions easily:

- What data am I collecting?
- Why am I collecting the data?
- What will I do with the data?
- How long will I keep the data for and how will I remove it?
- Where will I store the data?
- Who will have access to the data?

- Will I be sharing the data with anyone outside of Magic Me? Eg Funders, care homes/schools?
- Have I told the person who the data relates to that they have the right to ask us to:
    - Rectify any mistakes in the data
    - Provide them with a copy of the data we hold on them
    - Delete the data we hold on them (in certain circumstances we can override this request eg to fulfil our legal obligations)

Data collection and processing:

Personal data is processed on one or more of the following lawful bases:

- Consent: Data subjects have given clear consent for their personal data to be processed for specific purposes.
- Contract: Processing is necessary for the performance of a contract with the data subject or to take steps at the request of the data subject prior to entering into a contract.
- Legal Obligation: Processing is necessary to comply with a legal obligation.
- Vital Interests: Processing is necessary to protect the vital interests of the data subject or another person.
- Legitimate Interests: Processing is necessary for the legitimate interests pursued by Magic Me or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

For special categories of personal data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for identification purposes, health data, sex life data, sexual orientation data), Magic Me will do it's best to anonymise the data if at all possible. If for some legitimate reason we are unable to anonymise the data we will also meet one of the following special category conditions for processing under data protection law:

- The individual (or their parent/carer when appropriate in the case of a child or young person) has given explicit consent
- The data needs to be processed to perform or exercise obligations or rights in relation to employment, social security or social protection law
- The data needs to be processed to ensure the vital interests of the individual or another person, where the individual is physically or legally incapable of giving consent
- The data has already been made manifestly public by the individual
- The data needs to be processed for the establishment, exercise or defence of legal claims
- The data needs to be processed for reasons of substantial public interest as defined in legislation

- The data needs to be processed for health or social care purposes, and the processing is done by, or under the direction of, a health or social work professional or by any other person obliged to confidentiality under law
- The data needs to be processed for public health reasons, and the processing is done by, or under the direction of, a health professional or by any other person obliged to confidentiality under law
- The data needs to be processed for archiving purposes, scientific or historical research purposes, or statistical purposes, and the processing is in the public interest

Magic Me collects and processes personal data for the following specified and legitimate purposes, and indicated lawful bases, including:

- Programme Delivery (consent, contract, legal obligation, vital interest):
    - Providing services to beneficiaries
    - Meeting monitoring and evaluation requirements set by funders
    - Purposes of safeguarding children and adults at risk (beneficiaries)
- Funding (contract, legal obligation, legitimate interest):
    - Processing donations
    - Securing funds and grants
    - Maintaining donor and funder records
- Marketing activities (consent, legitimate interest):
    - Communicating updates to stakeholders and the wider community
    - Delivering events and activities promoting the organisation
- Operational activities (consent, contract, legal obligation, vital interest):
    - Managing employee records executive people processes (i.e. payroll)
    - Managing volunteer activities and communications
    - Fulfilling legal, accounting, and reporting obligations.

Magic Me collects the following personal and sensitive personal data:

- Personal data:
    - Contact information
        - Name, address, email address, phone number
    - Demographic information
        - Age/DOB
    - Financial information
        - Donation forms, employee payroll records, bank account details
    - Professional information
        - Job title, employer details, professional qualifications
- Sensitive personal data
    - Demographic data
        - Race/ethnicity, sexual orientation

- People management/health data
  - Medical conditions, allergies, disability status
- Criminal history
  - Convictions, offences

Further information on the personal data Magic Me collects can be found in the relevant data impact assessments. The sources of this personal data are indicated on Magic Me's Data Map.

Data retention:

As standard, personal data is retained for 6 years from the end of the financial year the data relates to in line with multiple statutory financial and HR retention periods. Occasional deviations to this retention period are highlighted within individual Data Impact Assessments per project and/or business function. At the point this policy is reviewed, an annual data review will be conducted by the DPO with Google Workspace data older than 6 years being archived automatically by Penelope and data on platforms such as Xero and Beacon being reviewed and archived, deleted or redacted as appropriate.

Data subject rights:

Magic Me respects the rights of individuals regarding their personal data, including:

- Right of access: Data subjects have the right to obtain confirmation of whether or not their personal data is being processed and access to their personal data.
- Right to rectification: Data subjects have the right to request the rectification of inaccurate or incomplete personal data.
- Right to erasure: Data subjects have the right to request the erasure of their personal data under certain circumstances.
- Right to restriction of processing: Data subjects have the right to request the restriction of processing of their personal data under certain circumstances.
- Right to data portability: Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and transmit it to another controller.
- Right to object: Data subjects have the right to object to the processing of their personal data under certain circumstances, including processing for direct marketing purposes.
- Right to File a Grievance: Data subjects have the right to file grievances with a regulatory body regarding the processing of their personal data, ensuring access to justice and regulatory oversight.
- Awareness of automated decision-making: Data subjects have the right to know when data is processed automatically and to be aware of the processes and safeguards in place to protect individuals' rights and interests.

Requests from data subjects (known as Data Subject Access Requests or DSARs) to exercise their rights will be promptly acknowledged and responded to in accordance with applicable data protection legislation. Magic Me commits to acknowledging receipt of DSARs within 72 hours and providing a response within 28 days of the date of receipt.

Staff are asked to respond to a data subject access request confirming receipt only (no details of when or how Magic Me will action the request should be referenced). The details of the request should then be provided to the DPO who will action the request. In the event of the absence of the DPO the request should be flagged to a member of the Senior Leadership Team. The DPO can extend the response time of the request in the event that the request encompasses a significant amount of data.

Data security:

Magic Me implements appropriate technical and organisational measures to ensure the security of personal data against unauthorised or unlawful processing and accidental loss, destruction, or damage. Security measures include:

- Devices are Bitlockered (laptop hard drives are encrypted)
- Devices are Microsoft Intuned with security features such as password lockout policy and devices have disabled auto-run
- Devices have location services enabled
- Devices have Windows Hello enforced for logon; simple passwords are blocked
- Devices enforce screen lock timeout
- Devices enforce sleep on battery power
- Magic Me uses NordPass Password Manager to protect passwords and to allow administrators to restrict access to passwords in the event that a device is lost or stolen
- MagicMe's data is in Google Drive - Google has AES-256 encryption for data at rest and in transit
- Staff learning and development programme (see section below)

Magic Me's IT support provider is responsible for the monitoring of these features and the update of devices. Automatic updates are rolled out regularly to staff devices with enforced restarts after a certain period to ensure these features are maintained.

Data sharing and transfers:

Magic Me only shares personal data with third parties when necessary for the purposes for which it was collected, and appropriate safeguards are in place to ensure the security and confidentiality of the data.

Magic Me shares personal data with the following third parties for the indicated purposes under the linked data protection agreements.

- Beacon Publishing Ltd - funder, donor, stakeholder, artist management and occasional promotional activities
    - Privacy Policy
- Due Diligence Checking - managing DBS applications
    - Privacy Policy
- Mailchimp (The Rocket Science Group LLC) - marketing and updates to our community
    - Data Processing Addendum
- Xero - personnel records, payroll, storage and processing of supplier and customer payment information and contact details
    - Data Processing Addendum
- Google Drive - storing and processing
    - Data Processing Addendum
- 34SP (website hosting service) - recruitment and job application data
    - Terms and conditions (see section 10)

International transfers of personal data are conducted in compliance with applicable data protection legislation. Google, Mailchimp and Xero have servers based in the US and personal data processed with these organisations is covered by the Data Protection (Adequacy) (United States of America) Regulations 2023.

Data breach management:

In the event of a data breach involving personal data, Magic Me has procedures in place to assess and mitigate the risks, notify the relevant supervisory authority and affected individuals, and take necessary actions to prevent similar incidents in the future. This process is documented here. In the event of a data breach, Magic Me will notify the ICO within 72 hours of becoming aware of it.

Continuous improvement of this policy:

This policy will be reviewed on an annual basis. Colleagues are invited to feedback on the policy for its improvement and encouraged at training sessions and team meetings to identify any elements of the policy that may need further clarification or strengthening.