Policy name:	Data Protection Policy
Author:	Ben Butcher, Head of Operations
Approved by:	FAR Committee
Approved date:	30/12/25
Review date:	30/12/26

Revision number	Date	Details of Change(s)
1	21/10/24	
2	30/12/25	• Updated to comply with Data (Use and Access) Act 2025. • Simplified to be easier to for staff to use including a summary.

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, the UK General Data Protection Regulation (GDPR) and the Data (Use and Access) Act 2025. 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)
    - Complaints Policy
- Useful links:
    - Information Commissioner's Office (ICO) support for organisations

Values:

We work collaboratively, inclusively, creatively, and thoughtfully. We apply these values by being thoughtful in data capture, collaborating with stakeholders on their obligations, and being creative about reducing the quantity of data we hold.

EDI & Anti-racism:

Magic Me is an inclusive, anti-racist environment and places particular sensitivity on data related to inclusivity such as race and ethnicity. On principle, we anonymise or pseudonymise sensitive data wherever possible and only collect it when necessary for monitoring inclusivity or reporting.

Scope:

This policy applies to all personal data collected, processed, and stored for Magic Me activities by its employees, volunteers, contractors (including artists) and third parties.

Magic Me's Data Protection Officer (DPO) is the Executive Director (currently Ben Butcher) who can be contacted via dpo@magicme.co.uk.

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, and the right to file grievances with Magic Me (before contacting ICO).

Data security: Appropriate technical and organisational measures are implemented to ensure the security of personal data against unauthorised processing, loss, destruction, or damage.

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:

We adhere to the seven core principles of the UK GDPR: Lawfulness, Fairness, and Transparency; Purpose Limitation; Data Minimisation; Accuracy; Storage Limitation; Integrity and Confidentiality; and Accountability . We remain accountable for demonstrating compliance with these principles at all times.

Key tenets of good data protection practice:

Anyone processing data for Magic Me should be able to answer:

- What data am I collecting and why?
- How long will I keep it and where is it stored?
- Who has access and will it be shared externally?
- Have I informed the individual of their rights to rectify, copy, or delete their data?

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 its best to anonymise the data if at all possible. If we are unable to anonymise the data we will also meet one of the following special category conditions for processing under data protection law (these can be found at the top of this ICO page.

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:

Personal data is retained for 6 years from the end of the financial year it relates to, in line with statutory financial and HR periods. The DPO conducts an annual review to archive or delete data older than 6 years. 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:

Individuals have the following 'rights' over their data:

The Right	What it means	Staff Action
Access (Subject Access Requests [SAR])	They want a copy of everything we hold on them.	Notify the DPO immediately. Do not delete anything once a request is made.

Rectification	They want to fix an error (e.g., wrong phone number).	Update the record in Beacon immediately.
Erasure	They want to be "forgotten" and deleted.	Refer to DPO. We may need to keep some data for legal/financial reasons.
Object	They want us to stop emailing them.	Mark as "Opted Out" in Mailchimp/Beacon immediately.

We acknowledge Subject Access Requests (SARs) within 72 hours and provide a full response within 28 days 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 director. Under the 2025 Act, Magic Me may refuse or charge a fee for requests that are considered "vexatious or excessive".

Individuals also have the right to lodge a complaint regarding how their data is handled. Below is a headline complaints process (for further information see our complaints policy):

- Submission: Contact the DPO (dpo@magicme.co.uk) with details of the concern.
- Investigation: The DPO will investigate the matter and provide a formal response within 30 days.
- Resolution: We will outline the steps taken to rectify the issue.
- Escalation: If unsatisfied, the individual may escalate the complaint to the Board or the ICO.

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 but are not limited to :

- Devices are Bitlocker encrypted
- Access control is managed by two-factor authentication, Windows Hello, and NordPass Password Manager.

- MagicMe's data is in Google Drive - Google has AES-256 encryption for data at rest and in transit

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.

The use of AI is restricted to Google Gemini AI. Because Gemini is integrated into our Google Workspace, it is "private by design." Data you type into Gemini stays within Magic Me and is not used to train public AI. Staff should never upload personal data (such as participants lists) or unredacted, highly sensitive case notes (such as safeguarding files) into Gemini AI without DPO approval.

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) (USA) Regulations 2023.

Data breach management:

Magic Me will assess and mitigate any data breach, notifying the ICO and affected individuals within 72 hours of becoming aware of the breach. The process for handling breaches is documented here.

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.

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.