



LEICESTER MAGIC CIRCLE

Data Handling Policy

How the Leicester Magic Circle stores, protects and manages personal data

1. Purpose

This policy sets out the practical arrangements by which the Leicester Magic Circle handles personal data in its day-to-day operations. It is an internal document for committee members. It sits alongside the Circle's Privacy Notice, which explains to members and prospects how their data is used.

2. Data controller and responsibility

The Leicester Magic Circle is the data controller. The Interim Secretary is the named data protection lead responsible for day-to-day compliance. The Treasurer holds financial records and is responsible for the security of those records.

Role	Responsibility	Named person
Data protection lead	Day-to-day compliance, subject access requests, privacy notices, enquiry log	Scot Jerram, Interim Secretary
Financial records	Subscription records, payment data, standing order information	Barry Martin, Treasurer
Committee oversight	Approving this policy and any material changes to data practices	Executive Committee

3. What data we hold and where

Data type	Where held	Access
Membership register	Password-protected spreadsheet or document held by Interim Secretary	Interim Secretary. Treasurer for financial data only.
Enquiry / prospect log	Password-protected spreadsheet held by Interim Secretary	Interim Secretary only
Subscription payment records	Held by Treasurer (bank records, standing order schedule)	Treasurer only
Application forms (physical or digital)	Scanned and stored securely by Interim Secretary. Originals shredded after scanning.	Interim Secretary
Email correspondence	Stored in the Circle's email account (scot@leicestermagiccircle.org)	Interim Secretary
Committee minutes	Circulated to Executive Committee; stored by Interim Secretary	Executive Committee members



4. Data security requirements

Electronic data

- All files containing personal data must be password-protected.
- The Circle email account (scot@leicestermagiccircle.org) must use a strong password, changed at the start of each secretary's tenure.
- Personal data must not be stored on shared drives or services (such as Google Sheets) without appropriate access controls.
- Devices used to access Circle data must be password-protected and not shared with other household members for Circle purposes.

Physical data

- Application forms and any physical documents containing personal data must not be left unattended.
- Physical documents should be scanned and the originals shredded after processing.
- Membership lists must not be circulated in printed form without a clear purpose and must be collected back after use.

Data shared at meetings

- Attendance at committee meetings where personal data is discussed is restricted to Executive Committee members.
- Minutes should not include more personal data than is necessary for the record.

5. Retention and deletion

Data must not be kept longer than necessary. The retention periods below apply:

Data type	Retention period	Action at end of period
Current member records	Duration of membership + 3 years	Delete or anonymise
Lapsed member records	3 years from last contact	Delete if no re-engagement
Prospect / enquiry records	12 months from last contact	Delete if no application made
Financial / subscription records	6 years (HMRC requirement)	Securely delete
Email correspondence	3 years	Delete routine correspondence; retain significant decisions
Application forms	3 years from application date	Securely delete

The Interim Secretary will conduct an annual review of data held and delete records that have exceeded their retention period. This should be completed each year before the AGM.

6. Subject access and other rights requests

Any member, prospect or former member may submit a request to exercise their rights under UK GDPR (see Privacy Notice, Section 7). The following process applies:

1. Request received by Interim Secretary via email or letter.
2. Identity of the requestor verified before any data is shared.
3. Response provided within one calendar month of receipt.



4. If the request is complex or numerous, the period may be extended by two months — the requestor must be notified within the first month.
5. Log the request and outcome in the data protection record.

If you receive a subject access request or any other rights request, notify the Interim Secretary within 24 hours. Do not attempt to respond independently. The legal deadline is one month from receipt.

7. Data breaches

A data breach is any incident where personal data is accidentally or unlawfully destroyed, lost, altered, disclosed or accessed without authorisation. Examples include: sending an email to the wrong person, losing a physical membership list, or having the Circle email account compromised.

6. Any suspected breach must be reported to the Interim Secretary immediately.
7. The Interim Secretary assesses the severity and likelihood of harm to individuals.
8. If the breach is likely to result in a risk to individuals' rights and freedoms, it must be reported to the ICO within 72 hours of becoming aware of it.
9. Affected individuals must be notified without undue delay if the breach is likely to result in a high risk to their rights and freedoms.
10. All breaches must be logged, even if they do not meet the reporting threshold.

8. Changes to this policy

This policy will be reviewed annually by the Executive Committee and updated as required. Any material changes to how we handle personal data must be reflected in the Privacy Notice and communicated to members.