



THE MAZE GROUP CIC

Data Protection Policy

Issued: May 2025

Version: 2.0

Policy Approval

Approved By	Board of Directors
Date	31 May 2025

Issue and Revision Log

Issue	Date Issued	Date for Review
1.0	June 2023	June 2025
2.0	May 2025	May 2027

Contents	
1. Purpose	1
2. Scope	1
3. Definitions	1
4. Data Protection Principles	1
5. Lawful Basis for Processing.....	1
6. Rights of Data Subjects	1
7. Data Security	2
8. Data Sharing and Third Parties.....	2
9. Data Retention	2
10. Breach Notification.....	2
11. Responsibilities	2
12. Training and Awareness	2
13. Policy Review.....	2

1. Purpose

The purpose of this policy is to ensure that The MAZE Group CIC processes personal data in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. We are committed to protecting the rights and freedoms of individuals in respect of their personal data.

2. Scope

This policy applies to:

- All personal data processed by The MAZE Group CIC.
- All staff, volunteers, trustees, contractors, and anyone acting on behalf of the organisation.
- All data subjects whose personal data is collected, stored, processed, or shared by the organisation.

3. Definitions

- **Personal Data:** Any information relating to an identified or identifiable person.
- **Special Category Data:** Sensitive personal data such as health, ethnicity, religion, and criminal records.
- **Data Subject:** The individual whose data is being processed.
- **Processing:** Any operation performed on personal data (collection, use, storage, deletion).
- **Data Controller:** The organisation that determines the purposes and means of processing personal data.
- **Data Processor:** Any third party that processes data on behalf of the controller.

4. Data Protection Principles

The MAZE Group CIC is committed to upholding the following UK GDPR principles:

1. Lawfulness, fairness, and transparency
2. Purpose limitation – data is collected for specific, explicit, and legitimate purposes.
3. Data minimisation – only the data necessary for the stated purposes is collected.
4. Accuracy – data is kept accurate and up to date.
5. Storage limitation – data is kept no longer than necessary.
6. Integrity and confidentiality – data is processed securely.
7. Accountability – we take responsibility for, and can demonstrate, compliance with these principles.

5. Lawful Basis for Processing

We will only process personal data where a lawful basis under the UK GDPR applies, including:

- Consent
- Contractual necessity
- Legal obligation
- Vital interests
- Legitimate interests
- Public task (if applicable)

Special category data will only be processed with explicit consent or where another specific condition is met under Article 9 of the UK GDPR.

6. Rights of Data Subjects

The MAZE Group CIC will ensure individuals can exercise their rights, including:

- The right to be informed
- The right of access (subject access request)
- The right to rectification
- The right to erasure (right to be forgotten)
- The right to restrict processing
- The right to data portability

- The right to object
- Rights in relation to automated decision-making and profiling (if applicable)

7. Data Security

We take appropriate technical and organisational measures to secure data, including:

- Use of password-protected systems and encrypted communications
- Secure file storage and access controls
- Regular training on data protection and cyber security
- Secure disposal of paper and digital records

8. Data Sharing and Third Parties

- Data will only be shared where legally required or with consent.
- Data sharing agreements will be in place with third-party processors.
- Any international data transfers will comply with UK GDPR rules.

9. Data Retention

Personal data will be retained only for as long as necessary for the purposes collected. A data retention schedule is maintained and reviewed regularly.

10. Breach Notification

- All staff, contractors or volunteers must report any actual or suspected data breaches immediately to the designated Data Protection Lead.
- Breaches will be assessed and, if necessary, reported to the Information Commissioner's Office (ICO) within 72 hours.

11. Responsibilities

- Data Protection Lead: Oversees data protection compliance, policies, and incident management.
- All Staff, Contractors and Volunteers: Must understand their responsibilities and follow data protection procedures.

12. Training and Awareness

All staff, contractors and volunteers will receive appropriate data protection training and refresher sessions to ensure ongoing compliance.

13. Policy Review

This policy will be reviewed bi-annually or in response to significant changes in legislation, guidance, or organisational structure.