



# Mind Bearer Ltd.

# Data Protection Policy

**Last Update:** Wednesday, 29 April 2026

**Scope:** Mind Bearer Ltd.

**Issued by:** Practice Manager

**Contact:** [policy@mindbearer.com](mailto:policy@mindbearer.com)



## Table of Contents

<b>1. DOCUMENT CONTROL</b>	<b>4</b>
<b>2. GLOSSARY</b>	<b>5</b>
<b>3. INTRODUCTION</b>	<b>6</b>
<b>4. SCOPE</b>	<b>6</b>
<b>5. DEFINITIONS</b>	<b>6</b>
<b>6. DATA PROTECTION PRINCIPLES</b>	<b>6</b>
<b>7. LAWFUL BASIS FOR PROCESSING</b>	<b>6</b>
<b>8. DATA COLLECTION</b>	<b>7</b>
<b>9. USE OF DATA</b>	<b>7</b>
<b>10. DATA STORAGE AND SECURITY</b>	<b>7</b>
<b>11. DATA SHARING</b>	<b>7</b>
<b>12. RETENTION OF RECORDS</b>	<b>7</b>
<b>13. DATA SUBJECT RIGHTS</b>	<b>8</b>
<b>14. CONFIDENTIALITY AND ANONYMISATION</b>	<b>8</b>
<b>15. DATA BREACHES</b>	<b>8</b>
<b>16. THIRD-PARTY PROCESSORS</b>	<b>8</b>
<b>17. REMOTE AND ONLINE COUNSELLING</b>	<b>8</b>
<b>18. TRAINING AND AWARENESS</b>	<b>9</b>
<b>19. POLICY REVIEW</b>	<b>9</b>





# 1. Document Control

<b>Document Name</b>	MB Data Protection Policy
<b>Document Owner</b>	Practice Manager
<b>Document Location</b>	MB Policies Repository
<b>Last Reviewed</b>	29 April 2026
<b>Next Review Date</b>	29 April 2027
<b>Version Released</b>	V 1.0

<b>Name</b>	<b>Date</b>	<b>Version</b>	<b>Approved By</b>	<b>Comments</b>
Data Protection	29 April 2026	V1.0	Richard Nettleship	Initial Version



## 2. Glossary

Term	Description



## 3. Introduction

This Data Protection Policy outlines how Mind Bearer Ltd ("the Company") collects, uses, stores, and protects personal data in the provision of counselling services. It ensures compliance with the UK GDPR and the Data Protection Act 2018, with particular attention to the handling of special category data.

## 4. Scope

This policy applies to:

- All counsellors, therapists, and clinical staff
- Administrative and support staff
- Contractors and third-party service providers
- Any systems or processes handling personal data

## 5. Definitions

Personal Data: Any information relating to an identifiable individual

Special Category Data: Sensitive data including health and mental health information

Processing: Any operation performed on personal data (e.g., collection, storage, use)

## 6. Data Protection Principles

The Company adheres to the following principles:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

## 7. Lawful Basis for Processing

The Company processes personal data under the following lawful bases:

- Provision of Healthcare Services (including counselling)
- Explicit Consent (where required)
- Legal Obligations (e.g., safeguarding)



- Special category data is processed under Article 9(2)(h) (healthcare provision) and/or explicit consent where applicable.

## 8. Data Collection

Data collected may include:

- Client identification and contact details
- Medical and mental health information
- Session notes and treatment records
- Emergency contact details
- Data will be collected directly from clients unless otherwise justified.

## 9. Use of Data

Personal data is used for:

- Delivering counselling services
- Managing appointments and communication
- Safeguarding and risk management
- Legal and regulatory compliance

## 10. Data Storage and Security

Records are stored securely (locked cabinets or encrypted digital systems)

Access is restricted to authorised personnel only

Strong passwords and, where possible, multi-factor authentication are used

Devices must be secured and not left unattended

## 11. Data Sharing

Data may be shared only when necessary:

- With supervisors (anonymised where possible)
- For safeguarding purposes
- When required by law (e.g., court orders)
- Clients will be informed of data sharing unless doing so would increase risk.

## 12. Retention of Records

Adult client records are typically retained for 7 years after the end of therapy



Records relating to minors are retained until the client reaches age 25 (or 26 if 17 at end of therapy)

Retention periods may vary based on legal or insurance requirements

## 13. Data Subject Rights

Clients have the right to:

- Access their personal data
- Request correction of inaccurate data
- Request erasure (where applicable)
- Restrict or object to processing
- Lodge a complaint with the Information Commissioner's Office (ICO)
- Requests must be responded to within one month.

## 14. Confidentiality and Anonymisation

Client confidentiality is strictly maintained

Identifiable information is minimised in supervision and training contexts

## 15. Data Breaches

All data breaches must be reported immediately

Serious breaches will be reported to the ICO within 72 hours where required

Affected individuals will be informed where there is a high risk to their rights and freedoms

## 16. Third-Party Processors

Third-party services (e.g., booking systems, cloud storage) must be GDPR-compliant

Data Processing Agreements (DPAs) must be in place

## 17. Remote and Online Counselling

Secure platforms must be used for online sessions

Clients should be informed of any risks associated with digital communication

Sessions should be conducted in private environments



## 18. Training and Awareness

Staff will receive training on data protection and confidentiality

Regular updates will be provided on legal and regulatory changes

## 19. Policy Review

This policy will be reviewed annually or when changes in legislation or practice occur.