Data Protection Policy & Procedure

Contents

1. Purpose of the Policy

Mediation Buckinghamshire (MB) needs to collect and use certain types of personal information about the people who use our service, our volunteers, our donors and our staff. This personal data must be collected and dealt with appropriately whether collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the Data Protection Act 1998 and in the General Data Protection Regulations (GDPR) which applies in the UK from 25th May 2018.

Some of the data collected may be sensitive data, i.e. data which concerns a person's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or sexual life.

Data protection is an important part of MB's overall information security arrangements. This policy sets out the responsibilities of MB, its Trustee Board, staff, volunteers, and Suppliers to comply fully with the provisions of the GDPR.

2. Policy Definition

MB regards the lawful and correct treatment of personal data as very important to successful working, and to maintaining the confidence of those with whom we deal. MB already processes personal data in accordance with Data Protection legislation, and this will continue to be the case in relation to the GDPR.

MB is defined as a Controller for the purposes of the Data Protection legislation and GDPR because it collects and processes personal data. The GDPR applies to all data relating to, and descriptive of, living individuals - defined in the GDPR as 'personal data'. Individuals are referred to as 'data subjects. For further definitions, please refer to Terms, Abbreviations and Acronyms in Section 9.

3. Disclosure

MB may share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Individual/Service User will be made aware in most circumstances how and with whom their data will be shared. There are circumstances where the law allows MB to disclose data (including sensitive data) without the data subject's consent.

These are:

- Carrying out a legal duty or as authorised by the Secretary of State

- Protecting vital interests of an Individual/Service User or other person
- The Individual/Service User has already made the information public
- Conducting any legal proceedings, obtaining legal advice or defending any legal rights
- Monitoring for equal opportunities purposes – i.e., race, disability or religion
- Providing a confidential service where the Individual/Service User's consent cannot be obtained or where it is reasonable to proceed without consent: e.g., where we would wish to avoid forcing stressed or ill Individuals/Service Users to provide consent signatures.

4. Scope

This policy applies to MB Trustee Board, staff, volunteers and Suppliers and to all items of personal data that are created, collected, stored and/or processed through any activity of MB.

5. Responsibilities

MB is required to adhere to the six principles of data protection as laid down in the GDPR, which means that information must be collected and used fairly, stored safely and not disclosed to any other person unlawfully. The principles relating to the processing of personal data require that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals.
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
- accurate and, where necessary, kept up to date; Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The GDPR further requires that the Controller shall be responsible for, and be able to demonstrate compliance with, these principles.

6. Lawful Processing

The lawfulness of processing conditions defined in the GDPR are as follows:

- Consent of the data subject
- Processing is necessary for the performance of a contract with the data subject or to take steps to enter into a contract
- Processing is necessary for compliance with a legal obligation
- Processing is necessary to protect the vital interests of a data subject or another person
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

.

For the rest of the services we provide, the legal basis for processing is Performance of a Contract as we must have certain personal data in order to deliver our services efficiently, safely and securely to Individuals/Service Users. This may include special categories of data.

MB holds personal data on staff for management purposes, for which the legal basis for processing is Compliance with a Legal Obligation.

MB holds personal data on donors and supporters for Gift Aid or accounting/tax purposes, for which the legal obligation is Compliance with a Legal Obligation and for marketing, research, maintenance and monitoring purposes for which the legal basis is Legitimate Interest.

MB may also maintain details of individuals who have objected to Direct Marketing, often referred to as a suppression list. For this we need to maintain enough personal information to ensure we meet and adhere to individual's objections in future.

7. Fair & Transparent Processing

Under the 'fair and transparent' requirements of the first principle, MB is required to provide individuals/service user with a 'privacy notice' to let them know what we do with their data.

Privacy notices are published on MB's website and are therefore available to most individuals e.g., volunteers, donors, supporters, who have access to the internet.

However, a number of our Service Users may not have access to the Internet, and their first contact with MB will be via a telephone. When collecting personal data, MB will ensure that the Individual/Service User:

- Clearly understands why the information is needed
- Understands what it will be used for and what the consequences are should the Individual/Service User decide not to give consent to processing
- As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
- Is, as far as reasonably discernable, competent enough to give consent and has given so freely without any duress
- Receives sufficient information on why their data is needed and how it will be used

8. Procedure

8.1. Data Collection

MB will ensure that personal data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form.

When collecting data based only on consent, MB will ensure that it can reasonably demonstrate that the Individual/Service User has consented to processing of his or her personal data.

8.2 Security of Processing

MB must process personal data securely by means of appropriate technical and organisational measures. Maintaining data security means guaranteeing the confidentiality, integrity, availability and resilience of the personal data, defined as follows:

- Confidentiality means that only people who are authorised can access the data.
- Integrity means that personal data should be accurate and suitable for the purpose for which it is processed.
- Availability means that authorised users should be able to access the data if they need it for authorised purposes.
- Resilience means that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process.

Information and records relating to service users will be stored securely and will only be accessible to authorised staff, volunteers and in some cases, Suppliers.

Procedures and technologies have been put in place to maintain the security of all personal data from the point of collection to the point of destruction, taking into account the state of the art and the costs of implementation. These procedures and technologies will be reviewed on a regular basis to ensure these are fit for purpose.

Personal data may only be transferred to a third-party processor if that party agrees to comply with those procedures and technologies, or if that party implements adequate procedures and technologies itself.

Data will be stored for only as long as it is needed or required by statute and will be disposed of appropriately.

8.3 Personal Data Breach

MB must protect the personal data that it holds against unauthorized or unlawful processing, accidental loss, destruction, and damage of data. MB makes every effort to avoid personal data breaches, however it is possible that mistakes will occur on occasions. Examples of personal data breaches could include:

- Loss or theft of data or equipment
- Inappropriate access controls allowing unauthorized use
- Equipment failure

- Unauthorised disclosure (e.g., mail sent to the incorrect recipient)
- Human error
- Hacking attack

If a data protection breach occurs, the Data Protection Officer is required in most circumstances to report this as soon as possible to the Information Commissioner's Office, and not later than 72 hours after becoming aware of it.

8.4 Individuals' Rights

All Individuals/Service Users have rights under the GDPR. These are:

- *The right to be informed* – this right requires MB to provide 'fair processing information', typically through a privacy notice.
- *The right of access* – generally referred to as a subject access request, this right allows individuals to confirm the accuracy of personal data and check the lawfulness of processing to allow them to exercise rights of rectification, erasure or objection as necessary. MB must provide the information free of charge within one month.
- *The right to rectification* – individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
- *The right to erasure* – sometimes referred to as the 'right to be forgotten', this right is to enable an individual to request the deletion or removal of personal data where there is no reason for its continued processing.
- *The right to restrict processing* – this gives individuals the right to 'block' or suppress processing of personal data. MB can store the data, but not further process it, and is allowed to retain enough information about the individual to ensure that the restriction is respected in the future.
- *The right to data portability* – this allows individuals to obtain and reuse their personal data across different services e.g. in a .CSV file.
- *The right to object* – for MB, this gives individuals the right to object to direct marketing or to processing for purposes of scientific/historical research and statistics.
- *Rights in relation to automated decision making and profiling* – this provides safeguards to individuals against the risk that a potentially damaging decision is taken without human intervention.

8.5 Suppliers
MB will ensure that its Suppliers conform to Data Protection legislation and GDPR by inspection of their Terms and Conditions, and any relevant contractual terms.

MB confirms that, in respect of any personal data it holds about the Supplier and its employees MB is bound by the terms of this Policy.

9. Compliance
MB will comply with its obligations under the Data Protection Act 2018 and the GDPR.

MB will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection, where no Data Protection Officer is in place then their role will be carried out by the Chief Executive Officer.
- Everyone processing personal data understands that they are contractually responsible for following good data protection practice
- Everyone processing personal data is appropriately trained to do so
- Everyone processing personal data is appropriately supervised
- Anybody wanting to make enquiries about handling personal data knows what to do
- It deals promptly and courteously with any enquiries about handling personal data
- It describes clearly how it handles personal data
- It will regularly review and audit the way it holds, manages and uses personal data
- It regularly assesses and evaluates its methods and performance in relation to handling personal data

All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them.

MB will, through appropriate management and strict application of criteria and controls:

- Observe fully conditions regarding the fair collection and use of personal data
- Meet its legal obligations to specify the purposes for which personal data is used

- Collect and process appropriate personal data, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
- Ensure the quality of personal data used
- Ensure that personal data is not transferred abroad without suitable safeguards
- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
- Set out clear procedures for responding to requests for information

MB will ensure that this policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998 and the GDPR.

10. Review of Effectiveness

The implementation and effectiveness of this policy and the requirements that stem from it will monitored by the Trustees at least annually, to identify any trends which may need further action.

The Chief Executive Officer (CEO) is responsible for ensuring appropriate reporting to the Trustee Board and will recommend and implement any improvement actions required.

11. Terms, Abbreviations and Acronyms

Controller – The natural or legal person, public authority, agency or other body which, (either alone or jointly with others) decides what personal information MB will hold and how it will be held or used.

Data Protection Act 1998 – The UK legislation that provides a framework for responsible behaviour by those using personal information.

Data Protection Officer – The person(s) responsible for ensuring that MB follows its data protection policy and complies with the Data Protection Act 1998 and the GDPR.

Individual/Service User – The person whose personal information is being held or processed by MB for example: a client, an employee, or supporter.

Explicit consent – is a freely given, specific and informed agreement by an Individual/Service User in the processing of personal information about her/him. Explicit consent is needed for processing sensitive data.

GDPR – The General Data Protection Regulation which applies in the UK from 25th May 2018.

Notification – Notifying the Information Commissioner about the data processing activities of MB, as certain activities may be exempt from notification.

The link below will take to the ICO website where a self-assessment guide will help you to decide if you are exempt from notification:
http://www.ico.gov.uk/for_organisations/data_protection/the_guide/exemptions.aspx

Information Commissioner – The UK Information Commissioner responsible for implementing and overseeing the Data Protection Act 1998.

Processing – means obtaining/collecting, recording, holding, storing, organizing, aligning, copying, transferring, combining, blocking, erasing and destroying the information or data. It also includes carrying out any operation or set of operations on the information or data, including retrieval, consultation, use and disclosure.

Processor – means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Personal Data – Information about living individuals who are identifiable from that information or who could be identified from that information when combined with other data which MB holds or is likely to obtain. It does not apply to information about organisations, companies and agencies but applies to individuals, such as individual Silver Liners, volunteers or employees within MB.

Special Categories of data – refers to personal data revealing:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health
- Sex life or sexual orientation
- Identity through genetic or biometric data

Supplier – means any individual or company which provides services to MB under a contract.

12. Revision History and Approvals

Revision History

Date	Document Version	Document Revision History	Document Author / Reviser
05/01/2022	V1.0	Full review & Update	Anthea Beeks
19/01/2023	V2.0	Review and update	Anthea Beeks

Approvals

Date	Document Version	Approver Title	Approver Name & authorisation
27/01/2022	V1.0	Chair of Trustees	Phyllida Middlemiss
31/01/2023	V2.0	Chair of Trustees	Phyllida Middlemiss