bristol **mediation**

talk it through

Easton Business Centre
Felix Road, Easton
Bristol BS5 0HE
Telephone: 0117 9415379

Data Protection/Information Sharing Policy

Written by	MA/JC/JR
Board Approval	March 2016
Chair of Trustees	*B Musty*
Last Review	March 2017
Review M. Alderman - Trustee	May 2018
Next Review Date	May 2019

Registered Charity 100064; Company Number 2538842

Data Protection Policy - Introduction

Bristol Mediation needs to gather and use certain information about individuals.
These can include staff, clients, volunteers, trainers and any other people the organisation has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled and stored to meet data protection standards — and to comply with the law.

Why this policy exists
This data protection policy ensures Bristol Mediation:

- Adheres to its Confidentiality Policy
- Complies with data protection law and follow good practice
- Protects the rights of staff, volunteers, clients and partners
- Is open about how it stores and processes individuals' sensitive data
- Protects itself from the risks of a data breach

1) Data protection law

The EU General Data Protection Regulation (GDPR) and Data Protection Act 1998 (DPA) describes how organisations — including Bristol Mediation— must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

Definition of Key Terms under GDPR:

a) **Personal Data** is any information relating to an identified or identifiable natural person (**Data Subject**)
b) **Data subject** is an identifiable person who can be identified by an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to person's physical, physiological, genetic, mental, economic, cultural or social identity.
c) **Data Controller** is the organisation that 'determines the purposes', that decides to gather and use the information.
d) **Data Processors** carry out specific tasks on behalf of the data controller under contract and is generally not liable. There must be a binding contract; if there is not under the GDPR, it's a breach for which the controller is liable.

GDPR is underpinned by six important principles. These are:

1. Lawfulness, fairness and transparency.
2. Purpose limitations.
3. Adequate data minimisation
4. Accuracy.
5. Storage limitations.
6. Security, Integrity and confidentiality

Lawfulness, Fairness and Transparency:

a) Data shall be processed fairly, lawfully and with transparency. This means we must:
    i. have specified, explicit and legitimate grounds for collecting and using the personal data
    ii. not process data in a manner that is incompatible with those grounds
    iii. be transparent about how we intend to use the data and give Individuals appropriate privacy notices when collecting their personal data
    iv. handle people's personal data only in ways which is necessary and proportionate
    v. make sure we do not do anything unlawful with the data

Purpose limitation:

b) shall be obtained only for one or more of the purposes specified in the Act and shall not be processed in any manner incompatible with the purpose of those purposes. This means that we must:
   i. be clear from the outset about why we are collecting personal data and what we intend to do with it
   ii. comply with the Act's fair processing requirements – including the duty to give privacy notices to and seek consent from when appropriate Individuals when collecting their personal data
   iii. comply with what the Act says about notifying the Information Commissioner
   iv. ensure that if we wish to use or disclose the personal data for any purpose that is additional to, or different from, the originally specified purpose, the new use of disclosure is fair, lawful and justified on legitimate business grounds. Any new purpose which is not justified additional consent must be sought.

Adequate Data Limitation

c) shall be adequate, relevant and not excessive in relation to those purpose(s). This means that:
   i. we will hold personal data about an Individual that is sufficient for the purpose
   ii. we are holding it for in relation to that Individual
   iii. we do not hold more information than we need for that purpose

Accuracy

d) shall be accurate and, where necessary, kept up to date. This means that we must:
   i. take reasonable steps to ensure the accuracy of any personal data we obtain
   ii. ensure that the source of any personal data is clear
   iii. carefully consider any challenges to the accuracy of information and action any request from individuals to improve accuracy in a timely manner
   iv. consider whether it is necessary to update the information

Storage Limitation

e) should not be kept for longer than is necessary. This means that we should:
   i. review the length of time we keep personal data
   ii. consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it
   iii. securely delete information that is no longer needed for this purpose or these purposes
   iv. update, archive or securely delete information if it goes out of date

Security, Integrity and confidentiality

f) shall be processed in accordance with the rights of Individuals under the Act and GDPR. This means that the Individual has:

   i. a right of access to a copy of the information comprised in their personal data
   ii. a right to object to processing that is likely to cause or is causing damage or distress
   iii. a right to prevent processing for direct marketing
   iv. a right to object to decisions being taken by automated means
   v. a right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed
   vi. a right to claim compensation for damages caused by breach of the Act

g) shall be kept secure by the Data Controller (Director) who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information. This means that BM must:
   i. design and organise security to fit the nature of the personal data held and the harm that may result from a security breach
   ii. be clear about who in the organisation is responsible for ensuring information security
   iii. make sure we have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff

iv. be ready to respond to any breach of security swiftly and effectively.

h) not transfer data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals in relation to the processing of personal information. Of specific relevance to the Association:
    i. the European Commission has decided that certain countries have an adequate level of protection for personal data. Currently, the following countries: Guernsey, Isle of Man, Jersey are considered as having adequate protection.
    ii. Ensure that any data transferred to any organisation outside the EU has adequate levels of protection and that this is enshrined within service contract agreements

2) Policy scope

This policy applies to:

a) Any staff/volunteers doing any outreach work on behalf of Bristol Mediation both online and offline
b) All offices of Bristol Mediation
c) All staff and volunteers of Bristol Mediation
d) All contractors, suppliers and other people working on behalf of Bristol Mediation
e) It applies to all data that the agency holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include:
    a. Names of individuals
    b. Postal addresses
    c. Email addresses
    d. Telephone numbers
    e. Any other information relating to individuals

3) Data protection risks

This policy helps to protect Bristol Mediation from some very real data security risks, including:

a) **Breaches of confidentiality.** For instance, information being given out inappropriately. (See confidentiality policy)

b) **Reputational damage.** For instance, the agency could suffer if hackers successfully gained access to sensitive data.

4) Responsibilities

Everyone who works both paid and voluntary for or with Bristol Mediation has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Chair of Trustees** is ultimately responsible for ensuring that Bristol Mediation meets its legal obligations. The Chair is to be assisted at the trustee level by the nominated Data Protection lead.

The Chair and Data Protection lead is responsible for:

a) Monitoring legislative developments
b) Updating the board on Data protection issues and risks with support from the Director
c) Supporting the Director as data controller
d) Conducting data protection audits on policy and process

The **Director** is responsible for:

a) Keeping the trustees updated about data protection responsibilities, risks and issues.
b) Reviewing all data protection procedures and related policies, in line with an agreed schedule.
c) Arranging data protection training and advice for the people covered by this policy.
d) Handling data protection questions from staff, volunteers and anyone else covered by this policy.
e) Dealing with requests from individuals to see the data Bristol Mediation holds about them (also called 'subject access requests').
f) Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
g) Approving any data protection statements attached to communications such as emails and letters.
h) Addressing any data protection queries from journalists or media outlets like newspapers.
i) Where necessary, working with other staff to ensure any marketing initiatives abide by data protection principles

The **Administration Officer** is responsible for:

a) Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
b) Performing regular checks and scans to ensure security hardware and software is functioning properly.
c) Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

5) General Staff Guidelines

a) The only people able to access data covered by this policy should be those who need it for their work for or on behalf of Bristol Mediation.
b) Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
c) Bristol Mediation will provide training to all employees to help them understand their responsibilities when handling data.
d) Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
e) In particular, strong passwords must be used and they should never be shared.
f) Personal data should not be disclosed to unauthorised people, either within the agency or externally.
g) Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of, securely.
h) Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.
i) To consider and conduct data protection impact assessments when considering new projects or when data is being used for new identified purposesAny (or suspected) data breach must be raised as a matter of urgency with the director who should raise this with the Data Protection Trustee lead and Chair as soon as possible

6) Data Collection

Bristol Mediation will ensure that data is collected within the boundaries define this policy. This applies to data that is collected in person (face to face or over the telephone), electronically or by completing a form.

When collecting data, BM will ensure

a) That a legitimate ground for data collection under GDPR Article 6 or 10 has correctly been identified and attributed to personal and sensitive data
b) A clear timeline for the collection, purpose and deletion of data has been produced
c) A Data protection impact assessment has been conducted prior to collection of new data

When collecting data, BM will ensure, wherever possible, that the Individual:

a) clearly understands why the information is needed

b) understands what it will be used for and what the consequences are should the Individual decide not to give consent to processing (more relevant to sensitive health information)
c) understands who the data may be shared with
d) give the Individual the option to opt out of sharing the data
e) grants explicit written or verbal consent to collect and share sensitive data (health related information) whatever possible
f) is competent enough to give consent and has given so freely without any duress

The above points indicate that the Individual will have enough information for them to give Informed consent. Any concerns regarding competence should be referred to a health care professional. Only positive consent will be used as such BM will not use pre-filled boxes, implied forms or other opt out strategies.

7) Data Storage

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Director.

When data is stored on paper, it should kept in a secure place where unauthorised people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed.

a) When not required, the paper or files should be kept in a locked drawer or filing cabinet.
b) Staff, volunteers and any user of BM data should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
c) Data printouts should be shredded and disposed of securely when no longer required.
d) Data which can reasonably identify an individual must not be visible outside of office hours and must be securely stored (like names and addresses on whiteboards)

When data is stored electronically, it must be protected from unauthorised access, accidental deletion and reasonable protection from malicious hacking attempts:

e) Data should be protected by strong passwords that are changed regularly and never shared.
f) If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
g) Data should only be stored on designated drives and servers, and should only be uploaded to approved and secure computing services.
h) Servers containing personal data should be sited in a secure location, away from general office space.
i) Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
j) Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
k) All servers and computers containing data should be protected by approved security software and a firewall.

8) Data Use

a) When working with personal data, staff and volunteers should ensure the screens of their computers are locked when left unattended.
b) Personal data should not be shared informally, and hard copies of any sensitive data are discouraged. Any emails sent with sensitive data should be stored securely and password protected.
c) Data must be encrypted before being transferred electronically. The IT manager can explain how to send data to authorised external contacts.
d) Personal data should never be transferred outside of the European Economic Area.
e) Staff/volunteers should not save copies of personal data to their own computers. Always access and update the central copy of any data.

9) Data Accuracy

The law requires Bristol Mediation to take reasonable steps to ensure data is kept accurate and up to date. The more important it is that the personal data is accurate, the greater the effort Bristol Mediation should put into ensuring its accuracy.
It is the responsibility of all staff/volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

a) Data will be held in as few places as necessary. Staff/volunteers should not create any unnecessary additional data sets.
b) Staff/volunteers should take every opportunity to ensure data is updated. For instance, by confirming a client's details when they call.
c) Data should be updated as inaccuracies are discovered. For instance, if a client can no longer be reached on their stored telephone number, it should be removed from the database.

Data should be updated as inaccuracies are discovered. For example, if a telephone number no longer relates to the person on our database it should be removed.

10) Subject Access Requests

All individuals who are the subject of personal data held by Bristol Mediation are entitled to:

a) Ask what information is held about them and why.
b) Ask how to gain access to it.
c) Be informed how to keep it up to date..
d) Be informed how the agency is meeting its data protection obligations.

Subject access requests are any request for data and do not need to be identified by the individual as such.
If an individual contacts the agency requesting any information, this is called a subject access request.
Subject access requests do not have to take a particular format but staff/volunteers if asked should instruct the person to email it to the appropriate address making it clear that it's a subject access request.

The data controller will very the identity of the individual before releasing any information. Only information related to that individual will be released unless there is a suitable authority in place.

11) Data Sharing

In certain circumstances, GDPR allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances Bristol Mediation will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board, in particular the Chair, Legal and Data protection Lead.

It is recognised that Bristol Mediation will have to share personal data with external agencies, and organisations. Under GDPR there is an obligation on Bristol Mediation to ensure that this data is properly protected when provided to external processors. To give effect to this and protect Bristol Mediation the processors data protection policies must be considered before any data is exchanged.

12) Providing information

Bristol mediation aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, Bristol Mediation has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request or on the Bristol Mediation website.