January 2019

Data Protection Policy

This document is relevant to:	
Staff	✓
Volunteers	✓
Trustees	✓

1. Introduction & Background

Dorset Mind is committed to compliance with all national UK laws in respect of personal data, and to protecting the rights and privacy of individuals whose information the organisation collects in accordance with the General Data Protection Regulation and the UK Laws that implement it (**Data Protection Legislation**).

The purpose of the Data Protection Legislation is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge.

This Data Protection Policy (referred to as this **Policy**) is designed to ensure that Dorset Mind complies fully with Data Protection Legislation and that personal data is fairly, lawfully and transparently processed.

Dorset Mind is registered with the Information Commissioner's Office and Anna Windett (Trustee) is the individual in charge of GDPR compliance.

2. Scope

The Data Protection Legislation applies to all personal data throughout its lifespan, from the point of collection to its eventual destruction. Personal data includes any piece of information which enables the identification of a living individual, such as a name, contact details and health information. For the purposes of this Policy references to personal data shall include sensitive personal data or special categories of personal data unless stated otherwise.

The format in which the information is held is in most instances not relevant. If personal data exists in any form, whether electronic or in a paper-based filing system, it is covered by the Data Protection Legislation.

The Policy applies to all staff and volunteers of the organisation and third party contractors. You should familiarise yourself with this Policy, the Confidentiality Policy and Dorset Mind's other information policies and comply with their terms when processing personal data on our behalf.

3. Purpose and aims of this Policy

To protect the rights and privacy of living individuals who access Dorset Mind services, work for, or support Dorset Mind. To ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.

4. Policy Statement

Dorset Mind is registered with the Information Commissioner's Office (the **ICO**) to process certain information about staff, volunteers, third party contractors, clients and supporters in order to provide the following:

- Provision of Mental Health services
- Fundraising, campaigning and membership services
- Monitoring, evaluation and audit of service provision
- Training

When processing personal data in the context of your work with us, you must comply with the six principles of good practice identified in Article 5 of the GDPR. They say the following:

1. **Lawfulness & Fairness:** Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
2. **Purpose Limitation:** Personal data shall be 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.
3. **Data Minimisation:** Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
4. **Accuracy**: Personal data shall be 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.
5. **Storage Limitation:** Personal data shall be 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

6. **Security:** Personal data shall be 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.

In simple terms, this means we must collect and use personal data fairly, tell people how we will use their personal data, store it safely and securely and not disclose it unlawfully to third parties. We need to be careful that the information we collect is relevant and that we do not collect more information than we need for the stated purpose.

There are restrictions on the transfer of personal data outside the EEA and information should not be transferred outside of the UK unless it meets the requirements of the Data Protection Legislation. Any such transfers require approval from the individual in charge of GDPR compliance.

Partners and any third parties working with or for the organisation, and who have or may have access to personal data, will be expected to comply with the principles of this Policy. No third party may access personal data held by the organisation without having first entered into a third party agreement which imposes on the third party obligations no less onerous than those to which the organisation is committed and which gives the organisation the right to audit compliance with the agreement.

4.1 Data Collection

There are a number of teams at Dorset Mind who collect and process personal data. Many of these teams have different rules relating to what they do with the data. Staff should not contravene any of these rules. If you are unsure, please contact the individual in charge of GDPR compliance.

Data Minimisation is important to think about prior to the collection of any personal data and we should only collect information that is absolutely necessary.

Data owners must ensure that they have a lawful basis for processing personal data. Under the GDPR there are 6 lawful bases for processing non-sensitive personal data as follows; consent or as is necessary as part of a contract, to comply with a legal obligation, to protect the vital interests of an individual, to fulfil a public task or as part of the organisation's legitimate interests (provided the latter is balanced against the rights of the individual).

Stricter rules apply to sensitive personal data (or special categories of personal data), such as information about a person's health, ethnic origin or religious beliefs as well as information

about criminal offences. We can only collect this information under very limited circumstances – for example, the person has given explicit consent or it is necessary for specific reasons permitted by law. If in doubt, please contact the individual in charge of GDPR compliance who can assist.

4.2 How does it affect me?

The Charity could be fined if you use or disclose information about other people without their consent or reliance on other lawful grounds. In order to help keep personal data secure, you should take particular care when using the Internet, e-mail and the internal network or talking on mobile or landline telephones. You could be committing an offence if you steal or recklessly misuse personal data.

Special care must be taken with sensitive personal data (or special categories of personal data) such as information relating to race, ethnic origins, religious/political beliefs, health data, disabilities, sexual life, genetics, biometrics or trade union membership. Details of criminal offences or alleged offences must also be handled with special care.

Any breach of the Data Protection Legislation or this Policy will be dealt with under the Charity's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

4.3 Responsibilities under Data Protection Legislation

- Dorset Mind is a data controller under the Data Protection Legislation.
- The Management and all those in managerial or supervisory roles throughout the Charity are responsible for developing and encouraging good information handling practices within the organisation. The individual in charge of GDPR compliance in particular has direct responsibility for ensuring that the organisation complies with the Data Protection Legislation, as do Line Managers in respect of data processing that takes place within their area of responsibility.
- The individual in charge of GDPR compliance has specific responsibilities in respect of procedures such as the Subject Access Request procedure and is the first point of call for staff seeking clarification on any aspect of the Charity's data protection compliance.
- Compliance with the Data Protection Legislation is the responsibility of all members of Dorset Mind who process personal data.
- Members of the organisation are responsible for ensuring that any personal data supplied by them, and that is about them, to the Charity is accurate and up-to-date.

4.4 Individuals' Rights

Individuals have the following rights regarding data processing, and the data that is recorded about them:

1. The right to be informed about how we process their personal data
2. The right to access their personal data
3. To right to rectify their personal data
4. To right to have their personal data erased
5. The right to restrict processing
6. The right to have a copy of their personal data in a portable form
7. The right to object to direct to marketing and profiling
8. Rights in relation to automated decision making and profiling.

If you receive a request, you should forward it on to the individual in charge of GDPR compliance immediately.

Where a person requests access to their information, this is called a data subject access request or 'DSAR':

- Dorset Mind must usually respond within one month.
- The response must be in a permanent form, unless this is not possible or the individual agrees otherwise.
- Unintelligible terms must be explained.
- The data must not be changed between receipt of a subject access request and sending the information to the applicant, except for routine amendment of the data which would happen in any case.

There are some exemptions to the rights detailed above, the details of which are included in the Subject Access Rights procedure.
All DSARs are co-ordinated by individual in charge of GDPR compliance in conjunction with the relevant office/department.

4.5 Consent & Transparency

Personal data should not be obtained, held, used or disclosed unless the individual has given consent or there is another lawful basis that allows us to do so. The organisation understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified (by an affirmative action) their freely given agreement preferably in writing, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. See the Consent Policy for further information.

All Dorset Mind services should display or make available adequate privacy notices to clients explaining how Dorset Mind processes their information. We must provide privacy notices even if we do not need to ask for consent.

The Dorset Mind permissions library contains a list of permission statements that provide adequate Privacy notices, these statements must not be amended. If an additional statement is needed contact the individual in charge of GDPR compliance.

4.6 Security of Data

All staff are responsible for ensuring that any personal data which the organisation holds and for which they are responsible, is kept securely and is not disclosed to any third party unless that third party has been specifically authorised by the organisation to receive that information and has entered into a confidentiality agreement.

You must not remove personal data from Dorset Mind's premises either in electronic or paper form unless it is really necessary – for example, in cases where staff have to attend external meetings, etc. In instances where data is taken out of the Dorset Mind premises, such data must be fully encrypted and password protected. If data is in a paper format, the staff member handling such data should ensure that any names of people and/or any information that could lead to identification of subject individuals is transported and stored securely.

Personal data pertaining to supporters or beneficiaries should be stored securely on Dorset Mind systems and not be taken out of the office in paper or electronic format at any time unless a risk assessment has been undertaken and this is approved by individual in charge of GDPR compliance.

Staff must comply with the information handling requirements in Dorset Mind's Confidentiality Policy.

4.7 Disclosure of Data

Dorset Mind must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All staff should exercise caution when asked to disclose personal data held on another individual to a third party.

All third party requests to provide data must be supported by appropriate paperwork and specifically authorised by the Data Protection Officer.

4.8 Retention & Disposal of Data

Personal data may not be retained for longer than it is required, e.g. after a member of staff has left the Charity, it may not be necessary to retain all the information held on them. Some data will need to be kept for longer periods than others. Dorset Mind's retention and data disposal procedures will apply in all cases.

Personal data must be disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and in line with Dorset Mind's Record Retention Procedure.

Personal data may need to be kept for a certain period of time under other legislation such as accounting or tax laws. In such cases reasonable measures must be taken to ensure it is kept securely in accordance with industry standards.

Duplicate copies of personal data should not be kept as doing so increases the risk of that data being compromised.

4.9 Data Protection by Design

Personal Data must be protected and the Data Protection Legislation requires data protection to be taken into account whenever a new system or process is introduced or where a system or process is changed that involves processing personal data.

Data Protection Impact Assessments (DPIA) must be completed and approved by the individual in charge of GDPR compliance for any significant changes to how personal data is processed at Dorset Mind that are likely to result in a high risk to individuals and where any new technologies or systems are used. A DPIA is required, in particular, if:

- installing a new CCTV system
- carrying out automated decision-making where it may have a legal or similarly significant effect on an individual
    - carrying out a project involving large-scale processing of sensitive data or information relating to criminal convictions

4.10 Working with third party partner organisations

All Dorset Mind projects funded in partnership with other third party organisations should include within the contractual agreement a clear statement as to the extent to which Dorset Mind and the third party partner organisation is responsible for compliance with Data Protection Legislation (as data controller and / or data processor) and the respective obligations of Dorset Mind and the third party partner organisation with regard to data protection.

For example, where Dorset Mind shares personal data with a third party provider, such as a mailing house providing direct marketing services, there must be a contract setting out that Dorset Mind is the data controller and the third party is a data processor and the respective obligations of both parties under the Data Protection Legislation.

All new contracts with third party partners or providers with whom we are sharing personal data need to be authorised by individual in charge of GDPR compliance.

In addition, any external parties such as contractors with access to personal data during the course of their work will be required to conform to Dorset Mind confidentiality standards and this Policy and must demonstrate their agreement in writing.

Dorset Mind works with Mind on occasion and other local Minds, they are charities in their own right but we are affiliated to them through a membership agreement. Mind will have its own data protection policies and procedures in place.

4.11 Personal Data Breaches

The Information Breach Policy provides details about the steps that need to be taken when a Personal Information Breach occurs – for example, loss of a memory stick or accidental disclosure of personal data to a third party. Where the breach is likely to result in a risk to individuals, the individual in charge of GDPR compliance must notify the Information Commissioners Office at the soonest possible time and within 72 hours of Dorset Mind becoming aware of the breach. If the risk of the breach is high the individuals who are affected must be informed directly and without undue delay.

You should report all breaches to your manager, IT and the individual in charge of GDPR compliance who will decide how to respond to the breach and whether it needs to be notified – see the Information Breach Policy for more information.

4.12 Anonymisation

Anonymisation is the process of removing information that could lead to an individual being identified (for example, names and other obvious identities which reveal the identity of the individual). Personal data should be anonymised whenever it is practical and appropriate to do so. Anonymising personal data significantly reduces the risks to individuals if that information is compromised.

Where personal data is collected and needs to be retained for statistical purposes, but it no longer needs to be attributable to an individual it should be anonymised at the earliest opportunity.

Fully anonymised data can be difficult to achieve in some situations. Where this is the case it is still good practice to partially anonymise the data to lower the chance of it identifying an individual.

Due to the sensitive information that we often receive via surveys, the Dorset Mind survey monkey account should only be used for anonymous surveys. If a survey needs to be completed a more secure survey application must be used under the advice of the Service Delivery Manager.

5. Roles and Responsibilities

5.1 Senior Management

Overall responsibility for compliance with Data Protection Legislation rests with the CEO. The CEO is responsible for making sure that the Data Protection function is fully resourced to meet the needs of the Charity.

5.2 Quality and Compliance

The individual in charge of GDPR compliance and CEO will monitor and review the operation of this Policy and receive feedback from departmental leads. They will report to the Dorset Mind Executive Team and Board.

Operational adherence to this Policy is delegated to the individual in charge of GDPR compliance, who is responsible for:

- understanding and communicating obligations under the Data Protection Legislation
- identifying potential problem areas or risks
- producing effective procedures
- notifying and annually renewing notification to the Information Commissioner

5.3 Managers and Heads of Departments

Managers and Heads of Departments are responsible for promoting data protection awareness and compliance with Data Protection Legislation and this Policy within their teams. This includes working with the individual in charge of GDPR compliance to respond to data subject access requests from members of the public or staff. Heads of Departments and/or Managers are also responsible for making sure that all members of staff in their teams have been accorded the necessary data protection training.

Managers must ensure that all new staff take the mandatory data protection training and review this Policy as part of their induction.

5.4 All Staff, Volunteers and Trustees

It is the responsibility of all staff, volunteers and trustees to ensure they understand and act in accordance with this Policy and Data Protection Legislation.
Staff, volunteers and trustees should also ensure that they keep the individual in charge of GDPR compliance updated if they become aware of any proposed changes or changes to the ways in which personal data is being processed by their team.

Staff, volunteers or trustees found to be acting contrary to this Policy may be subject to disciplinary action. This is because any breach of the Data Protection Legislation could result in Dorset Mind facing legal action.

Responsibilities
The Chief Executive is responsible for managing this policy and overseeing its implementation. Line managers are responsible for implementing the policy within their areas of work, and for overseeing adherence by staff and volunteers. Every member of staff should take personal responsibility for conforming to it.

Associated Policies and Procedures

- Confidentiality Policy
- Archive and retention policy

The equality impact of this policy has been considered and Dorset Mind believes that it complies with its commitment to equality as stated in its Equality Policy

Policy Ownership

Policy Name	Version	Doc ref
Data Protection Policy	2.0	DATA PROTECTION POLICY

Policy Owner	Individual in charge of GDPR Compliance

Approval Status

Date adopted by Trustees	January 2019		
Date published	January 2019	Date for next review	January 2021

Document Control

Reviewers

Name	Position
Anna Windett	Trustee
Marianne Storey	CEO
Iain Saker	Trustee

Change History

Issue	Date	Author	Reason
1.0	Jan 16	Chris Price	New policy
2.0	Jan 19	Anna Windett	Update post GDPR