Data Protection Policy

1. Policy Statement

Derbyshire Mind is committed to being a responsible user of personal data and ensuring that the relevant legislation is adhered to at all times. This includes maintaining appropriate privacy and offering a high level of confidentiality to the people using its services, its employees, volunteers, members, those interacting via Social Media, suppliers and contractors.

We will ensure procedures are in place to fairly process data relating to individuals and take appropriate technical/security measures to safeguard this information.

This policy must be followed by all Derbyshire Mind paid employees and volunteers, who for the purposes of this document will be referred to as staff.

The purpose of this policy is to ensure that all staff are aware of their obligations and responsibilities when handling personal data within Derbyshire Mind.

All staff have a responsibility to be aware of and adhere to our policies and procedures. All breaches will be investigated and any deliberate or grossly negligent behaviour may render employees liable to disciplinary action, including dismissal for gross misconduct, or in the case of volunteers, contractors or suppliers a termination of our agreement.

2. Responsibilities

The Trustees of Derbyshire Mind have overall responsibility for data protection. On a day to day basis this responsibility will be implemented and administered by the Management Team and the organisational lead on data protection who is the Office Manager.

2.1 The Office Manager will:-

- co-ordinate policy matters relating to data protection and liaise with the Management Team to monitor arrangements for processing and sharing of data.
- deal with any questions from data subjects or from staff about how data is or should be used in the organisation.
- handle Subject Access Requests and any other request from a data subject to exercise their data protection rights.

2.2 The Management Team, in conjunction with all Supervising Managers, are responsible for:-

- ensuring that procedures and processes within their area of work promote good data protection practice.
- making sure that staff are aware of this policy and associated policies/procedures.
- ensuring that appropriate support and regular training is provided on data protection and confidentiality.
- recording & investigating incidents in collaboration with the CEO, monitoring and reviewing policies and procedures.

2.3 All staff have a personal responsibility for data protection and are required to:-

- assist the public to understand their rights and Derbyshire Mind's responsibilities in regard to data protection legislation.
- immediately report to their line manager any data breach, potential breach or 'near miss' they become aware of, regardless of how it occurred.
- report any incidents that may contravene the policy and procedures.
- inform their Line Manager immediately if they become aware of any impracticalities associated with or necessary additions to policies and procedures.

3. Data Protection Overview

The Data Protection Act 2018 and General Data Protection Regulation (GDPR) set out the legal standards for the use of personal information and how it may be obtained, held, used or disclosed. This legislation is intended to provide protection for individuals when data about them is held by organisations. It also gives individuals important rights in respect of their data.

3.1 Core Principles

We must comply with the six enforceable data protection principles:-

They state that data must be:-

- processed lawfully, fairly and in a transparent manner.
- obtained for specified, explicit and legitimate purpose and not be further processed in any manner incompatible with those 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 erase or rectify inaccurate personal data without delay.
- kept in a form which permits identification of data subjects for no longer than is necessary.
- processed in 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.

3.2 Personal Data

Personal data is defined as any information relating to an identifiable, living individual.

Someone is considered to be 'identifiable' if there is any way in which you could pick them out from another either directly or indirectly, even if you do not know their name. This would for example cover a photograph where a person is clearly distinguished or the user name of someone who is interacting online.

4. Processing of Personal Data

The legislation applies whenever personal data is processed. Section 4 (2) of GDPR defines this as:-

> *"any operation or set of operations which is performed on personal data or on any sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making it available, alignment or combination, restriction, erasure or destruction."*

This means that Derbyshire Mind has responsibility for complying with the data protection legislation from the moment at which personal data is obtained until it is finally destroyed or erased, even if it is not being actively used.

4.1 What Data Do We Hold and Why?

We have to have a lawful basis to process personal data. This must be one or more of:-

- Consent from the individual.
- A contract with the individual.
- A legal obligation.
- To protect a person's vital interests.
- To perform a public task.
- In the legitimate interests of Derbyshire Mind or someone else.

None of these six options is preferred; consent is not 'better' than any other. Derbyshire Mind will determine the lawful basis for processing whenever a service or activity is developed or reviewed.

We collect personal data in connection with specific activities, for example recruitment, employment, membership, use of our services, donations. The amount and type of information we process will vary and depend on type of interaction a person has with Derbyshire Mind.

4.2 Transparency

We must ensure that we are clear and transparent with regards to the data we process. This will be done in a number of ways:-

Derbyshire Mind:-

- identifies and documents what personal data is held by the organisation, on what grounds we hold it, where it has been obtained and who is it shared with.
- specifies where information is stored and for how long before deletion.
- has a number of privacy statements for different aspects of their work which are noted in associated policies, leaflets and via social media.

- ensures people interacting with the organisation and using our services are made aware of the information we hold about them, why we are collecting it, how they can access it and their rights under data protection legislation.

4.3 Data Quality and Retention

Our Retention and Disposal Schedule sets out our requirements and timeframes for the retention of data and all staff are responsible for adhering to this.

Staff must ensure that the data they collect or record is kept up to date, accurate and not held without a lawful reason or for longer than necessary. Unstructured data such as emails must comply with the six data protection principles whenever it contains information about identifiable individuals (even if their identity is obscured).

4.4 Security of Information

Derbyshire Mind will take all reasonable precautions to protect all personal data that we hold and process.

In particular, appropriate measures will be taken to ensure that 'data in transit' – whether by email or other electronic means, by post, or physically being moved from one place to another does not fall into the wrong hands or go astray.

All hard copies of personal data are stored securely with restricted access. All information held electronically will be protected securely in line with our Information Technology Policy and associated procedures.

Staff should not remove hard copies of personal data from Derbyshire Mind premises without prior consent from their Line Manager so that appropriate security measures can be put in place. Guidance should be obtained from the Office Manager, or member of the Management Team in these circumstances.

5. Disclosure of Information

Much of the personal data held by Derbyshire Mind is strictly confidential. Confidential personal data is never passed or disclosed to any third party without permission from the individual concerned, except as required by law or in exceptional cases where this is permitted by data protection legislation.

All staff are responsible for ensuring that personal data is held securely and not disclosed to anyone unless they are authorised to have access to that information. Staff should not allow anyone access to premises or equipment unless this has been authorised. If a staff member is unsure about any request then they should seek advice from their Line Manager and the Office Manager before disclosing data.

All disclosures of confidential or personal data should be recorded. These should include:-

- What data has been disclosed.
- Who it has been disclosed to.
- What is the reason for disclosure.
- Whether the individual's permission has been obtained.
- Whether the individual receiving the information has authorisation to access this information.

- What method has been used to disclose the information, eg, by e-mail, telephone, letter, etc.
- Were any measures taken to ensure that the information was transferred securely and if so what measures were used.

Derbyshire Mind will not give out information about any individual over the telephone or by e-mail unless it is satisfied that:-

- the data subject knows that this type of disclosure may be made (or that there is some over-riding reason for the disclosure).
- giving the information over the telephone or by e-mail is appropriate because of urgency or because the level of risk is low.
- the identity of the person making the request has been verified.
- the person making the request is authorised to have the information.
- Sufficient security measures are in place to protect the transfer of information (e.g. password protected documents, call back to ensure number is safe).

6. Accessing Information

All individuals have a right to know what information Derbyshire Mind holds about them and to make a 'Subject Access Request' verbally or in writing. We will also ensure that individuals can easily get answers to any questions they have about why and how their information is used.

Any staff member may find themselves the recipient of a Subject Access Request. This must be acknowledged and then passed immediately to the Office Manager, who will manage the process or the CEO in their absence.

If an individual becomes aware that their personal information which we hold contains errors, omissions or inaccuracies then they are entitled to ask us to rectify the information or, in some cases, to erase or destroy it. This request should be directed to the staff member responsible for the management of that data.

No charge will be made for the first subject access request from any individual to Derbyshire Mind. Derbyshire Mind reserves the right to make a charge for additional copies of data that has been provided or for subsequent unreasonable requests.

See the Access to Records Policy and Procedures for more details.

7. Actual and Potential Donors, Members, Supporters

Any marketing or publicity material which invites people to contact Derbyshire Mind will state that any data supplied will be used for these purposes and will give data subjects the opportunity to opt out. Where data items are optional (e.g. telephone numbers, e-mail addresses), this will be made clear.

No details of individuals will be passed to other organisations for marketing or fundraising purposes.

The organisation will respect the additional restrictions on marketing by phone, fax, e-mail, text message and on the web which are set out in the Privacy and Electronic Communications (EC Directive) Regulations 2003 and other relevant legislation.

General Provisions Applying to all Data Subjects

Whilst the procedures and practices outlined in this policy relate to the overall application of data protection legislation, there are a number of associated policies and procedures which relate to the specific processing and management of data in certain areas of the organisation or in relation to specific work we undertake (e.g. Mental Capacity Act). In addition to this, we are also bound by other legislation which may at times affect how the data protection legislation should be applied.

Please note that this policy should be read in conjunction with the Confidentiality Policy and Procedures, Access to Records Policy and Procedures and A Guide to Keeping information Secure When Working Remotely or From Home.