Data Protection Policy

Policy Statement

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

The purpose of this policy is to ensure that Derbyshire Mind complies with relevant, current legislation including Data Protection Act 2018, UK GDPR, and that all staff are aware of their obligations and responsibilities when handling personal data.

This policy covers all personal data, including physical and digital data, special category and criminal offence data, and information from all data subjects including staff, volunteers and service users.

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

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 organisational lead on data protection who is the Head of Central Services.

The Head of Central Services 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.

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, including mandatory training and refreshers.
- recording and investigating incidents in collaboration with the Head of Central Services, monitoring and reviewing policies and procedures.

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.
- complete and refresh as required mandatory data protection training.
- inform their Line Manager immediately if they become aware of any impracticalities associated with or necessary additions to policies and procedures.

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.

Core Principles

The UK GDPR sets out seven key principles:

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

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.

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.

Lawfulness, fairness and transparency

The lawful bases for processing data are:

- Consent
- Contractual obligation
- 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.

'Consent' is only used where we can offer real choice and control over how the data is used. Where consent is used, it will be for specific data about which the person has been fully informed and which they give freely. Consent will be recorded in writing, with information given as to how consent can be withdrawn.

We collect personal data in connection with specific activities, for example recruitment, employment, membership, use of our services, and donations. The amount and type of information we process will vary and depend on the type of interaction a person has with Derbyshire Mind. We tell individuals about the data we collect and how it is used through privacy notices and verbal explanation at point of collection.

Additional bases are required when processing special category/criminal offence data. Special category data is racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, a person's sex life or sexual orientation.

Article 9 of the UK GDPR prohibits the processing of special category data except for the following conditions:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law) + DPA Schedule 1 condition
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law) + DPA Schedule 1 condition
(h) Health or social care (with a basis in law) + DPA Schedule 1 condition
(i) Public health (with a basis in law) + DPA Schedule 1 condition
(j) Archiving, research and statistics (with a basis in law) + DPA Schedule 1 condition

We process criminal offence data only where absolutely necessary for the purpose we have identified, and where we have identified an appropriate DPA Schedule 1 condition from the following:

1. Employment, social security and social protection	13. Journalism in connection with unlawful acts and dishonesty	27. Anti-doping in sport
2. Health or social care purposes	14. Preventing fraud	28. Standards of behaviour in sport
3. Public health	15. Suspicion of terrorist financing or money laundering	29. Consent
4. Research	17. Counselling	30. Vital interests
6. Statutory and government purposes	18. Safeguarding of children and individuals at risk	31. Not-for-profit bodies
7. Administration of justice and parliamentary purposes	23. Elected representatives responding to requests	32. Manifestly made public by the data subject
10. Preventing or detecting unlawful acts	24. Disclosure to elected representatives	33. Legal claims
11. Protecting the public against dishonesty	25. Informing elected representatives about prisoners	34. Judicial acts
12. Regulatory requirements relating to unlawful acts and dishonesty	26. Publication of legal judgments	35. Administration of accounts used in commission of indecency offences involving children
		37. Insurance

Purpose limitation

Personal data is collected for specified, explicit and legitimate purposes and is not further processed in any manner incompatible with those purposes, which are recorded on our Record of Processing Activities and reviewed annually, or when a service or activity is reviewed.

Data Minimisation

Data capture processes are designed to ask only for data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

Staff are required to ensure that data they collect and hold is kept up to date, that data subjects may easily advise of inaccuracies or changes in their personal data, and that inaccuracies are erased or rectified without delay.

Storage Limitation

Data is retained for no longer than is necessary for the purposes for which the personal data is processed. Retention periods are noted on our Record of Processing Activities and Retention and Disposal Schedule. Disposal is overseen by the Data Protection Lead.

Integrity and confidentiality (security)

Derbyshire Mind will take all reasonable precautions to protect all personal data that we hold and process. Data protection impact assessments are carried out where required or where deemed necessary.

Staff are required to take measures to protect personal data on a daily basis including:

- Taking care of hard copy data on desks, when using printers and copiers and when posting
- Locking screens when away from desk
- Keeping passwords secure
- Sending electronic documents securely by encryption or password protection
- Shredding documents no longer required

Derbyshire Mind has technical measures in place to ensure that electronic data is secure and accessible in the event of incidents, as set out in our IT Policy. This includes Cyber Essentials and Cyber Essentials+ accreditation and periodic penetration testing.

Data Sharing

Derbyshire Mind will only share data where it is fair, necessary and proportionate and where there is a secure means of doing so. Where appropriate, data sharing agreements will be put in place to explain the specific aims, why data sharing is necessary to achieve those aims and the benefits hoped to be brought through sharing. Staff will be given appropriate training and access to records and systems to ensure that agreements are adhered to.

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 Head of Central Services 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).

Accountability

Our processing activities are documented in a Record of Processing Activities (ROPA). This Data Protection Policy shows how Derbyshire Mind aims to be a responsible user of personal data and ensures that the relevant legislation is always adhered to. Data protection is integrated into business and processing activities by design and DPIAs will be carried out for uses of personal data that are likely to result in high risk to individuals' interests.

Individual rights

All individuals have:

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision-making including profiling

Any staff member may find themselves the recipient of a request from an individual to exercise their rights including Subject Access Requests. Any such requests must be acknowledged and then passed immediately to the Head of Central Services, who will manage the process, or to the CEO in their absence.

Subject Access Requests will be processed in line with the Subject Access Request process. 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.

Personal Data Breaches

The Data Breach Policy and Procedure sets out the actions to be taken in the event of a breach or a near miss. Any staff who becomes aware of a data breach should contact their line manager immediately.

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 into mailing lists and opt out at any point thereafter. 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.

Review and monitoring

The Head of Central Services will monitor compliance with and effectiveness of this policy and related policies through spot checks that are undertaken annually. This policy will be reviewed every two years.