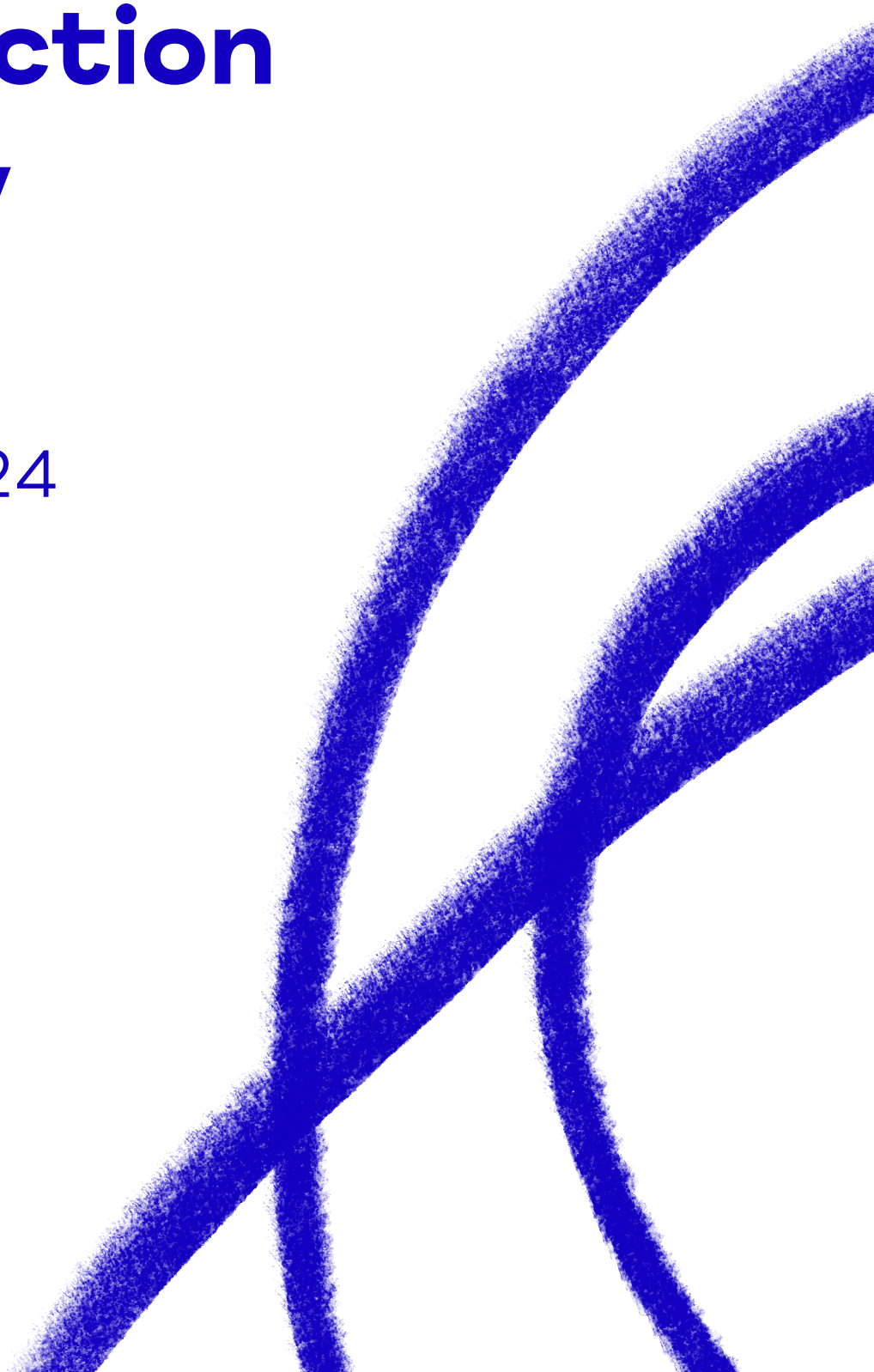
mind in Bradford

Data Protection Policy

Version 3
March 2024



Title	Data Protection Policy
Version	3
Date first published	September 2020
Previous review dates	June 2023, March 2024
Next review date	March 2027
Review schedule	This policy will be reviewed every 3 years.
Responsibility	Board of Trustees
Responsibility for development, review and implementation	CEO, Executive and Senior Leadership Team and Operational Service Team.
Description	Provides protection to our data and protect sensitive information.
Target audience	All staff, volunteers, the Board of Trustees, clients, students on placement with Mind in Bradford, visitors to Mind in Bradford, our funding bodies, job and volunteer applicants and third-party providers
Accessibility	Staff: People HR Volunteers: People HR Clients and others: On request If you would like this policy in another format, such as large print or audio, please request one by contacting us on 01274 730815 or at email admin@mindinbradford.org.uk
Associated policies	Client Code of Conduct Client Involvement and Engagement Policy Data Protection Policy Privacy Policy Volunteer Policy Safeguarding Adults Policy Safeguarding Children Policy Complaint Policy Conflict of Interest Policy

	Trustee Recruitment Policy Volunteer Policy In addition, supported by the following Procedures or Guides: DNAR Protocol Information Security Processes Data Quality Processes Records Management Processes Information Breach Processes Subject Access Requests Processes Information Systems Guide for Staff and Volunteers

Purpose of policy and statement

This is our policy and statement of the purposes for which we hold and process personal data about our clients, employees and others who work for us in accordance with our statutory obligations including the EU General Data Protection Regulation ("GDPR"). We will deliver our legal obligations through our Information Governance procedures.

The objective is to ensure that data is:

- Held securely and confidentially.
- Obtained fairly and lawfully.
- Recorded accurately and reliably.
- Used effectively and ethically.
- Shared and disclosed appropriately and lawfully.

We will be open and transparent with clients and those who lawfully act on their behalf in relation to their care and treatment.

We will adhere to our duty of candour responsibilities as outlined in the Health and Social Care Act 2012.

We will establish and maintain policies to ensure compliance with the Data Protection Act 2018, Human Rights Act 1998, the common law duty of confidentiality, the General Data Protection Regulation and all other relevant legislation.

We will establish and maintain policies for the controlled and appropriate sharing of client and staff information with other agencies, taking account all relevant legislation and citizen consent.

Where consent is required for the processing of personal data we will ensure that informed and explicit consent will be obtained and documented in clear, accessible language and in an appropriate format. The individual can withdraw consent at any time through processes which have been explained to them and which are outlined in our Records Management Processes: Withdrawal of consent procedures. We ensure that it is as easy to withdraw as to give consent.

We will undertake / commission an annual review of our compliance with legal requirements. Data will be processed in a manner that ensures appropriate security of the personal data under GDPR. We uphold the personal data rights outlined in the GDPR.

Definitions

- "Company" means Mind in Bradford.

- "data" means information which is stored either: electronically (whether on a computer, a removable drive or any other electronic device) or in a paper-based filing system which is structured and can be browsed by criteria, regardless of whether that filing system is dispersed across multiple locations.

- "data controller" means a person (whether an individual or a corporate body) which determine the purposes for which, and the manner in which, any personal data is processed.

- “data processor” means a person who processes personal data on behalf of a data controller, and does not in any way determine how or why data is processed.

- “data subject” means a living individual to whom personal data relates. A data subject need not be a UK national or resident. Note that all data subjects are protected by the GDPR.

- “ICO” means the Information Commissioner’s Office, the UK regulator for data protection law.

- “personal data” means any data (including but not limited to text, statistics, images and videos) relating to a living individual that either is identified in that data or is directly or indirectly identifiable from that data, for example only by reference to an identifier such as a name, a unique identification number, location data, an online identifier or username, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person, regardless of whether that data is fact or opinion.

- “processing” means any activity that involves use of personal data. It includes but is not limited obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

- “sensitive personal data” means personal data that: reveals the relevant person’s race or ethnic origin, political opinions, religious or philosophical beliefs (or beliefs of a similar nature), membership of a trade union is genetic data, or biometric data for the purpose of uniquely identifying the relevant person; concerns the physical health, mental health, sex life or sexual orientation of the relevant person; relates to the commission or alleged commission of a criminal offence; or relates to proceedings against the relevant person for a criminal offence or alleged criminal offence, including the disposal of those proceedings, or sentencing.

- “security breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal

data transmitted, stored or otherwise processed. Breaches must be reviewed and serious breaches must be reported to the ICO within 72 hours.

General obligations

Mind in Bradford acts as a data controller, which means that during the course of our activities, we will collect, hold and process information consisting of personal data including sensitive personal data about our clients, our employees, applicants for employment, self-employed contractors, agency workers and others who work for us.

The information, which may be held on paper, within computer files or on other media is subject to certain legal safeguards in accordance with GDPR and UK domestic legislation.

Due to our size, we have determined that we are not required to have a Data Protection Officer (DPO), as we do not process special categories of data on a large scale. Nonetheless, to ensure that every individual's data rights are respected and that there is the highest levels of data security and protection in our organisation, we have appointed a member of staff to the Data Security and Protection Lead role.

The Data Security and Protection Lead will report to the highest management level of the organisation. We will support the Data Security and Protection Lead with the necessary resources to carry out their tasks and ensure that they can maintain expertise.

This includes nominating a Senior Information Risk Owner (SIRO) at Board level. The SIRO's key responsibility is to manage information risks and to provide strategic leadership and guidance to the Data Security and Protection Lead from a senior level.

This policy and its supporting processes set out our rules on data protection and the legal conditions that must be satisfied in relation to any act taken in relation to personal information, including but not limited to the obtaining, handling, processing, storage, transportation and destruction of personal information.

Anyone processing personal data on behalf of the Company must only do so as instructed and in accordance with this policy and any other policy or procedure designed to ensure our compliance with our legal obligations.

Compliance with this policy and the organisation's procedures are mandatory and non-compliance will be taken seriously and may result in disciplinary action.

Employees, contractors and data processors may also have direct criminal liability, liability to the ICO and to data subjects for certain breaches under data protection laws.

If you consider that the policy and procedures have not been followed in respect of personal information about yourself or others, you should raise the matter with your line manager or the Data Security and Protection Lead.

Data protection obligations

Anyone processing personal data must comply with six data protection principles. The following summary is underpinned by the data protection procedures.

Mind in Bradford will ensure that it meets its obligations by implementing a comprehensive set of procedures which will support this policy. How the organisation will deliver assurance will be defined in the purpose and responsibilities statement.

This policy determines that personal data must be processed lawfully, fairly and in a transparent manner. This includes a requirement to;

- have a "legal basis" for processing personal data (see below);

- be transparent with data subjects, providing them specific information about the processing to be carried out before it is carried out; and to give data subjects certain rights in relation to their personal data.

1. **Specific Purpose**

Collected for a specific, explicit and legitimate purpose, and not further processed in a manner that is incompatible with those purposes.

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted GDPR or other relevant legislation.

This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose, or there is a new purpose, for which the data is processed, the data subject must be informed of the changed or new purpose before any processing occurs, and you must only use personal data for that changed or new purpose if it is compatible with the existing purpose.

2. Necessary for the Purpose

Adequate, relevant and limited to what is necessary in relation to the purpose for which it is processed.

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

If personal data later becomes excessive in relation to the purpose, it will need to be deleted unless there is another purpose (and associated legal basis) for keeping it.

3. Accuracy and relevance

Personal data must be accurate and kept up to date. Personal data which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards.

Inaccurate or out of date data that cannot be rectified should be destroyed.

Personal data should not be kept longer than is necessary for the purpose. Data should be destroyed or erased from our systems when it is no longer required for the purpose(s) originally notified to the data subject.

4. Security

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. The organisation has set out security and access requirements within its accompanying IG Procedures which support this policy.

We must maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if they agree to comply with our procedures and policies, or if they put in place adequate measures to ensure data security.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

• confidentiality means that only people who are authorised to use the data can access it.

• integrity means that personal data should be accurate and suitable for the purpose for which it is processed; and

• availability means that authorised users should be able to access the data if they need it for authorised purposes.

Personal data should therefore be stored on our central IT system instead of individual local files e.g. My Documents.

A summary of good practice for security procedures include:

• Access controls. Any stranger seen in entry-controlled areas should be reported.

• All staff should ensure that individual monitors do not show confidential information to passers-by and that they must lock or log off from their computer when it is left unattended.

• Security of data including secure lockable desks and cupboards. Desks and cupboards should be kept locked if they hold confidential information of any kind. (personal data is always considered confidential);

• Methods of data disposal. Paper documents should be shredded. Disks, USB sticks and CD ROMs should be physically destroyed using appropriate destruction methods when they are no longer required.

• Legal basis for processing

• Personal data must be processed lawfully, fairly and in a transparent manner.

5. Legal Basis

Under GDPR you must have a "legal basis" for processing. One such legal basis must apply to our processing of personal data for it to be lawful.

The GDPR (Article 6) allows processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations;

(d) to protect the Data Subject's vital interests;

(e) where the task is carried out in the public interest or in the exercise of official authority;

(f) other than by public authorities to perform their tasks, to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Statements/Notices or Fair Processing Notices.

6. Sensitive personal data

If processing sensitive personal data, more stringent rules apply (Article 9). These include:

a. the data subject has explicitly consented to processing for a specific purpose (explicit consent being a clear statement in words, rather than by action);

b. the processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the company or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or UK law;

c. the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. the processing relates to personal data which are manifestly made public by the data subject;

e. the processing is necessary for the establishment, exercise or defence of legal claims; and

f. the processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or UK law or pursuant to contract with a health professional and subject to certain conditions and safeguards.

Data subject rights requests

Right to access

Data Subjects have rights when it comes to how we handle their Personal Data. These include:

a. a right to receive a copy of their personal data which the company holds; and details of:

i. the purpose for processing;

ii. the categories of data processed;

iii. any recipients (or categories of recipients) to whom the personal data has been disclosed;

iv. the envisaged period for processing;

v. the existence of the right to request rectification or erasure;

vi. the source of the information (if not from the data subject themselves);

vii. any automated decision making, including meaningful information about the logic involved, and the significance and envisaged consequences of such decisions; and

viii. the safeguards put in place if the personal data has been transferred outside the European Economic Area;

b. The right to complain to the ICO

c. In limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine-readable format.

It is a legal requirement to ensure that subject rights requests are responded to within a month of the request.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your line manager and the Data Security and Protection Lead.

Right to rectification

We must rectify any inaccurate information held by us at the request of the data subject. This includes having incomplete personal data completed. This does not affect our primary obligation to keep personal data accurate and up-to-date.

Right to erasure

We must erase personal data at the request of the data subject, but only in limited circumstances, namely where:

a. the personal data is no longer necessary for the purpose it was processed;

b. we originally relied on consent, that consent is withdrawn and we have no other legal basis for processing;

c. the personal data is unlawfully processed; or

d. the personal data has to be erased for compliance with a legal obligation to which we are subject.

Right to restriction of processing

We must restrict (i.e. limit the scope of) our processing at the request of the data subject where:

a. the accuracy of the personal data is contested by the data subject, but only for a period enabling us to verify the accuracy of the personal data;

b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c. we no longer need the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; or

d. the data subject has objected to processing pursuant to the right to object to legitimate interests processing (see below), but only pending the verification of whether our legitimate grounds override those of the data subject (if they do not, we would then have to permanently restrict processing).

Record management and retention

In accordance with the organisations records management procedures records must be retained for the following periods. At the end of that period the records must be reviewed to determine whether the record is lawfully required for a further period or should be disposed of.

The categories of information which we will hold and the minimum time for which we will normally hold it will be as follows:

Application Form	Duration of Employment
References received	Duration of Employment
Payroll and tax information	6 years
Pension records	12 years after benefit ceases
Sickness and absence records	3 years
Annual leave records	1 year from end of employment
Unpaid leave/special leave records	1 year from end of employment
Annual appraisal/assessment records	5 years
Records relating to promotion, transfer, training, disciplinary matters	1 year from end of employment
Summary of record of service e.g. name, position held, date of employment	10 years from end of employment
Records relating to accident or injury at work	12 years
Client records	3 years from date of last entry
Members contact	3 years from date of last year of membership
Website cookie data	14 months from entry
Supporter	3 years from date of support

The purpose for which we hold any information about data subjects after the end of employment (as indicated in the above table) is for use solely for any residual employment related matters including but not limited to the provision of job references, processing applications for re-employment, matters relating to retirement benefits and allowing us to fulfil contractual or statutory obligations.

References

Providing a reference involves the disclosure of personal data of the individual who is the subject of the reference. So that we can ensure we protect our employees' data no references (whether to prospective employers or other institutions) should be given on behalf of the Company without prior authorisation from the Head of People and Culture

This Policy does not prevent any employee from giving a reference in a personal capacity but employees should make clear that such references are personal and not on behalf of the Company and, if the reference is given on paper, that neither the Company's name, address or logo appear on the paper.

Reporting a personal data breach

We may be required to report personal data breaches to the ICO and in certain instances, the Data Subject.

This should be done using the guidance provided in the Information Breach Processes document.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact your line manager and the Data Security and Protection Lead. You should preserve all evidence relating to the potential breach.

It is a legal requirement that the organisation must report serious data breaches to the ICO within 72 hours of the incident

Procedures and Guides supporting the Data Protection Policy

The Data Security and Protection Lead, working under the guidance of the SIRO, has direct responsibility for maintaining the policy and ensuring that Mind in Bradford is provided with advice and guidance on its implementation. The procedures and guidelines in this policy will be reviewed on a regular or upon significant internal/external changes and in conjunction with annual security audits.

In addition to the Data Protection Policy, we provide an Information Systems Guide for Staff and Volunteers our workforce. The guide is designed to support this policy and supporting processes by providing working guidance to all staff, volunteers, agency staff, seconded staff and contractors who deliver activity on behalf of Mind in Bradford. It explains how, in practical terms and using best practice advice:

• Information will be protected against unauthorised access.

• Confidentiality of information will be assured.

• Integrity of information will be maintained.

• Information will be supported by the highest quality data

• Regulatory and legislative requirements will be met.

• Business continuity plans will be produced, maintained and tested.

• Information security training will be available to all staff.

• All breaches of information security, actual or suspected, will be reported to, and investigated by the Data Security and Protection Lead.

The following process documentation also help ensure that the organisation meets its legal obligations under GDPR.

- Information Security Processes
- Data Quality Processes
- Records Management Processes
- Information Breach Processes
- Subject Access Requests Processes

Organisational responsibilities

Mind in Bradford Line Managers

Are responsible for ensuring that the Data Protection Policy is implemented within their group or department.

Mind in Bradford's IT provider(s)

Is responsible for ensuring that the information security policies and procedures are implemented across the organisation.

Employees and Volunteers

It is the responsibility of each individual working with or employed by the organisation to adhere to the policy.

Data Security and Protection Lead

Has been designated as the Information Technology and Information Governance lead for the organisation and has the following responsibilities:

- To ensure that all related policies and procedures are implemented, and the currency of them is maintained.
- To ensure that Mind in Bradford's approach to information handling is communicated to all staff.
- To coordinate the activities of staff given data protection, confidentiality, information quality and records management responsibilities.
- To liaise where required with the nominated Caldicott Leads to ensure that patient data is kept secure and that all data flows, internal and external are periodically checked against the Caldicott principles.
- To liaise where required with the nominated SIRO to ensure that leadership and guidance from Board level is sought and implemented.
- To ensure the SIRO and Board is adequately briefed on information risk issues.
- To monitor Mind in Bradford's information handling activities to ensure compliance with law and guidance.
- To ensure that training materials and guidance made available by Mind in Bradford and is taken up by staff as necessary to support their role.
- To ensure that all information assets have an assigned Information Asset Owner.

Senior Information Risk Owner (SIRO)

- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution.
- Provide a focal point for the resolution and / or discussion of information risk issues.

mind in Bradford

Your local mental health charity in Bradford, Airedale, Wharfedale and Craven