# Mind in Camden

## Data Protection Policy

### Background

This policy describes the measures we take to manage personal information. We want to make sure that we only collect what is relevant and ensure that we have secure measures in place to keep it safe and that we will keep it for no longer than necessary.

The purpose of data protection regulations is to give people rights in respect of their personal data and to give clear guidance to those who hold and process that information. All Mind in Camden staff and volunteers have a responsibility to follow the guidance provided.

Data protection applies to computerised and manual systems of information and the policy applies to all the personal data we process regardless of the media on which it is stored or whether it relates to past or present.

### Data protection definitions used in this policy

***GDPR:*** General Data Protection Regulations that came into force on 25th May 2018 as amended from time to time.

***Data Subject*****:** a living person about whom an organisation holds information.

***Personal Data:*** personal data is any information provided by individuals themselves or by a third party that can identify that person either on its own or with other information in our possession or likely to come into our possession.

***Special Category Data:*** relates to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health, sexual life, sexual orientation, biometric or genetic information. It is sensitive information that needs special protection and Mind in Camden cannot process it without a legal basis for doing so and must also meet specific conditions.

Under GDPR regulations information about criminal convictions or offences is dealt with in a similar way to special category information.

***Data Controller*****:** Mind in Camden as an organisation is a data controller because it determines what personal information is collected and how it is managed.

***Data Processor*****:** is usually a third party, such as another organisation, that may process information on behalf of a data controller (in this case, the Data Controller).

***Data Protection Officer:*** is legally required for certain organisations: those that are public bodies or process large amounts of data or types of data. We have been advised that it is not a current requirement for an organisation of Mind in Camden's size to have a Data Protection Officer. Instead the Chief Executive will be the named person to whom enquiries can be sent.

***Privacy Notice***: is a document that will be given to anyone who is asked to provide personal information. It explains what personal information we are collecting; how it will be used; how long we intend to keep it; how we store it and how we shall eventually dispose of it. The individual will be informed should we need to share it with others (third parties). They will also be advised of their rights to access their own personal data.

**Data Protection Principles**

Mind in Camden is responsible for and must be able to demonstrate compliance with the data protection principles listed below. Data must be:

- fairly and lawfully processed in a transparent manner
- collected for specified, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary
- accurate and kept up to date
- not kept for longer than is necessary
- processed in a manner that ensures appropriate security
- not transferred to another country without appropriate safeguards being in place
- made available to the individual and the individual must be allowed to exercise certain rights in relation to their personal data.

**The legal basis**

Any personal data that Mind in Camden collects will comply with one or more of the six legal bases required for processing:

- consent (further information on consent below)
- contract
- legal obligation
- vital interests
- public tasks
- legitimate interests

People will be informed about the legal basis or bases on which Mind in Camden is collecting their personal data and about the conditions for processing special category data where that applies i.e. why we ask for personal information and what we intend to do with it.

**Consent**

Mind in Camden cannot process personal information without consent. This may be in the form of signing a statement or other form of agreement, but it must involve positive action i.e. the individual from whom Mind in Camden seeks consent must actively give permission for their personal information to be processed; it won't be assumed, for example, we won't ask anyone to sign a

document that includes pre-ticked boxes, nor will we make assumptions based on silence or inactivity. If consent is given in a document that deals with other matters, then the consent will be kept separate from those other matters.

People must easily be able to withdraw consent to processing at any time and withdrawal must be promptly honoured by Mind in Camden.

If we later want to use someone's personal data for a completely different and incompatible purpose that they were not informed about when first given consent, we may need to ask for consent again.

We only ask for special category data or criminal conviction data for a particular purpose for which will have a legal basis and specific purpose. The privacy notice will explain why we collect it and how it will be used.

**Our purpose for processing personal data**
We hold information on many groups of people who associate with Mind in Camden which includes members, service users, employees, workers, volunteers, sessional contractors, suppliers, website users or other data subjects both past and present.

The nature of our work as a mental health organisation means that we may hold data that includes sensitive information about health, but we only hold relevant information that enables us to fulfil our obligations, for example:

- providing services
- complying with health & safety legislation
- not discriminating on grounds of race, disability, sexuality, faith or gender
- considering reasonable adjustments to the workplace for people with disabilities
- maintaining records for sickness and maternity pay
- safeguarding vulnerable service users; both adults and children

**Access to personal information (Subject Access Request)**
Anyone has the right to request information about the personal data that Mind in Camden holds about them. If they wish to do so they must put their request in writing with sufficient detail to enable the data to be identified. Mind in Camden must supply the information within one month of receiving the request

**Individual rights**
GDPR give certain rights in relation to Mind in Camden processing personal data. These are, the right:

- to withdraw consent to processing at any time
- to be informed
- to have access to their own information
- to rectification of inaccurate or missing data
- to prevent our use of personal data for direct marketing purposes
- to erasure
- to restrict processing

- to data portability
- to raise an objection
- in relation to automated decision making and profiling
- to prevent processing that is likely to cause damage or distress to themselves or to anyone else
- to be notified of a personal data breach which is likely to result in a high risk to someone's rights and freedoms
- to make a complaint to the supervisory authority

**Data Security**
Mind in Camden will develop, implement and maintain safeguards appropriate to our size, scope and business, available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). Mind in Camden will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

No-one who has access to personal data should disclose it outside Mind in Camden's procedures, or use it for their own purposes. This would be a disciplinary offence and possibly a criminal offence.

**Responsibilities**
Anyone at Mind in Camden who collects, records or uses personal information is responsible for the accuracy of their own work; for maintaining confidentiality and security and for reporting any errors or breaches of data security. If a data breach does happen, there is a procedure (described below) which must be followed.

**Third Party Sharing**
Mind in Camden will only transfer personal data to third party service providers that agree to comply with the required policies and procedures and who agree to put adequate measures in place as requested.

**Making a complaint**
If anyone wishes to make a complaint about a data protection matter at Mind in Camden, they should contact the Chief Executive, Brian Dawn
by email: bdawn@mindincamden.org.uk
or in writing to: Mind in Camden, Barnes House, 9-15 Camden Road, London NW1 9LQ
or by phone: 020 7911 0822.

People may also make a complaint about Mind in Camden to the Information Commissioner's Office. www.ico.org.uk . This website also has a lot of information and guidance about GDPR.

# Mind in Camden Data Protection Procedures

## I. Informed Consent

Whenever we collect personal data we need to make sure that the individual to whom it belongs is made aware of why we are collecting it (i.e. the legal basis for doing so); where it will be stored; how we will use it; how long we will keep it and how and when it will eventually be destroyed. People also need to be made aware of their rights over the information that they provide. We must issue a privacy notice to everyone from whom we collect personal data. Mind in Camden's privacy notices vary depending upon the nature and purpose of the services provided. We must also keep a record of the notice issued to enable us to demonstrate compliance with consent requirements

## 2. Confidentiality and Security

Everyone is responsible for safeguarding the personal information that they process. Everyone must take care to implement reasonable and appropriate security measures against unlawful or unauthorised processing of persona data and against the accidental loss of, or damage to, personal data. People must exercise particular care in protecting special categories of personal data and criminal convictions data from loss and unauthorised access, use or disclosure.

Therefore, everyone should follow all the procedures and technologies put in place to maintain the security of all personal data from the point of collection to the point of destruction. This includes managing paper records and following security protocols for managing computer records which are described fully in the ICT policy. The Confidentiality policy provides guidance on verbal communications about personal data.

## 3. Responsibilities for Personal Data Management

Responsibilities for safeguarding personal data in different areas of Mind in Camden's work is described below:

Service user records: team managers have responsibility for the safe keeping of service users' personal data and for determining what processes are needed to manage the service, including which people are allowed to process the information on a "need to know" basis. They are also responsible for managing data sharing with third parties and with other teams internally.

Enquirers: personal information given to Mind in Camden by the general public in order to obtain information or services mainly falls within the remit of the Resources Director who is supported by staff and volunteers.

Recruitment: job applicants will only be asked to supply information that is relevant to the role and sufficient to enable shortlisting decisions, as reasonably determined by Mind in Camden. Recruitment panels will follow the guidance in the Recruitment and Selection Policy to ensure that candidates are subject to a fair and confidential procedure. It will be made clear to candidates at the application stage that our work with vulnerable adults and children requires us to obtain Disclosure & Barring Service checks. The DBS policy gives more detail.

Candidates will also be made aware that if they are offered and accept a post it is a legal requirement for them to provide proof of their eligibility to work in the UK.

References given by Mind in Camden to outside parties: Mind in Camden is not obliged to give a copy of a reference given in confidence to the person who is the subject of the reference. Managers must follow Mind in Camden's policy on providing references.

References supplied to Mind in Camden: an employee does not necessarily have a right to access to information provided in a reference by a former employer that has been provided in confidence. An employee has access to data about themselves but this does not include the referee's opinion of them. The referee's consent should always be sought before allowing an employee to see a reference. The same principle applies to references provided for volunteers or sessional contractors.

Personnel records: are available on a "need to know" basis. Access is usually restricted to the individual and their line manager, but there are circumstances when the manager's manager will need access to information. The Finance Director also needs access to some information in order to fulfil payroll and pension responsibilities.

Volunteer records: personal data is processed on a "need to know" basis by the relevant team manager and the Resources Director.

**4. Retention Policy and Procedure**

Information will be kept only as long as it is required and will be destroyed securely and confidentially. Guidelines for retaining records are in a separate document. Managers are responsible for ensuring that records are checked regularly and Management Team will ensure that audits are carried out as required.

**5. Sharing Information with Third Parties**

A great deal of care needs to be taken in considering whether to share personal data with a third party or even between different teams at Mind in Camden. Consider the following risks when determining whether to share data: could anyone be damaged by it? Is the person likely to object? Might it undermine individuals' trust in the organisations that keep records about them?

Everyone must make sure they understand the requirements for sharing information with third parties, such as our service providers. Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place. We will enter a separate sharing agreement with every third party with whom we share data.

We will only share a Data Subject's data where we:

- have a clear reason for doing so and we must document this reason (with reference to the six legal bases above). The basis may be different for different groups of people whose information we hold.
- consider whether the objective could be achieved without sharing data or anonymising it
- only share information that is specific to the purpose.
- share information based on a "need to know" principle e.g. for the purposes of providing the contracted services
- be confident that sharing the Personal Data complies with the privacy notice given to the person and, if required, that their consent has been obtained
- make sure that the identity of the person requesting data has been verified and that it is within the remit of the rights listed above. (and not allow third parties to persuade us into disclosing personal data without proper authorisation)
- know that the third party has agreed to comply with the required data security standards, policies and procedures and has adequate security measures in place. Check whether a fully executed written contract that contains legally compliant third party processor/controller clauses has been obtained.
- make sure that if personal information is to be shared outside the UK that the transfer complies with any applicable cross-border transfer restrictions;
- finally, make sure the method of transferring the information is secure

Please see **Sharing Personal Data** (a separate document)

**6. Subject Access Requests**
Under GDPR people have certain rights over the information that we hold about them and we are obliged to respond within a set timeframe. Access requests should be forwarded to the Resources Director as soon as possible as we are obliged to respond within a fixed time limit.

Please see the separate document on **Subject Access Requests**

**7. Complaints**
Should anyone want to make a complaint in relation to our processing of their personal information, they can do so by contacting our Chief Executive, Brian Dawn. They may also make a complaint about Mind in Camden to the Information Commissioner. Details of how to do so are described in the policy above.

**8. Documentation**
GDPR requires us to document our processing activities, including keeping a register of data breaches. We need to document processing that is:

- Not occasional or
- Could result in a risk to the rights and freedoms of individuals or
- Involves processing special category data or criminal offence data

## 9. Personal Data Breach

Mind in Camden has a duty to report certain types of personal data breaches to the ICO within 72 hours of the breach taking place. We must also record every instance of a breach on an internal register.

A security breach means any action that might lead to accidental or unlawful destruction of personal data; loss, alteration, unauthorised disclosure of, or access to, personal data. It could be the result of accidental or deliberate causes. It includes loss by encryption by ransomware.

Breaches that are likely to have a significant impact must be reported, but others that cause little impact or harm may not need to be reported. Decisions must be made on a case by case basis. However, all breaches must be recorded internally and security improvements considered.

If a breach carries a high risk of adversely affecting individuals' rights and freedoms, they must also be informed as soon as possible. Adverse effects include loss of control over their personal data, loss of rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality, or any other significant economic loss or social disadvantage to the person concerned.

If anyone causes a breach or discovers that there has been a breach they must immediately report it to their manager. Members of Management Team will assess whether the breach is significant and determine what action to take. The breach must be reported to the Resources Director who is responsible for maintaining the data breach register.

## 10. Privacy Impact Assessments

Data Protection Impact Assessments (DPIA) must be carried out for certain types of processing that may result in a high risk to individuals' interests. It is also good practice to conduct a DPIA before starting any major new project.

DPIAs are required for services targeted at children and should be considered when processing sensitive information or vulnerable individuals.

The ICO provides tools for assessing risks, which once carried out, should ideally be published.

If a high risk is identified that cannot be mitigated, advice should be sought from the ICO.

## 11. Related policies:

- Absence – sickness
- Code of Conduct
- Complaints procedure
- Confidentiality
- Disclosure & Barring Service policies
- Disciplinary & Grievance procedures

- Information, Communication & Technology
- Protection of service users from abuse
- Recruitment & Selection
- References Policy
- Supervision & Appraisal
- Union Recognition agreement
- Volunteer Policy
- Whistleblowing