Mind in Camden

Data Protection Policy

Background
The requirements for data protection are complex and underpinned by a large body of legislation. The purpose of data protection is to give individuals rights about their personal data and to give clear guidance to those who hold and process that information.

Under the General Data Protection Regulation 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 Data Subjects and allow Data Subjects to exercise certain rights in relation to their personal data.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (accountability)

We provide further details on the principles of data protection below.

Data protection applies to computerised and manual systems of information.

This Data Protection Policy applies to all Personal Data we process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, service users, suppliers, website users or any other Data Subject.

This Data Protection Policy applies to all our Personnel. You must read, understand and comply with this Data Protection Policy.

Data Protection Roles

***Data Protection Officer*:** Mind in Camden is too small an organisation to warrant employment of a Data Protection Officer. Neither is there sufficient impartiality within the staffing structure to designate the role to a member of staff. Instead the Chief Executive will be a named person to whom enquiries can be sent.

***Data Controller*:** Mind in Camden as an organisation is a data controller.

Data covered by Data Protection
Data protection is concerned with personal data which means information that relates to a living person and identifies an individual either on its own or with other information in the organisation's possession or likely to come into its possession.

Special Category data
Certain information can only be held with the explicit consent of the individual. "Special Category data" relates to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sexual life, sexual orientation, biometric or genetic information.

Under GDPR regulations criminal convictions or offences are dealt in broadly the same way as a special category.

Note: as Mind in Camden is a mental health organisation, data held about service users is likely to include sensitive information about health.

Mind in Camden will only hold sensitive information that enables it to fulfil its obligations, for example:

- Providing its services
- Ensuring compliance 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

Purpose and use of data
People who are asked to provide personal information will be told what information is required, how it will be used, including disclosure to third parties, how stored and how long it will be kept before being securely destroyed. People will also be advised of their rights to access their personal data.

Access to information
Any individual has the right to request information that falls within data protection. The request must be in writing with sufficient detail to enable the data to be identified and information must be supplied within 30 days of receipt of the request

Conditions required for requesting and using personal data
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 which legal basis or bases their personal data is being collected and the conditions for processing special category data where that applies.

Consent
A Data Subject consents to the processing of their personal data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action, so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

When processing Special Category Data or Criminal Conviction Data, we will usually rely on a legal basis for processing other than explicit consent or consent if possible. Where Explicit Consent is relied on, you must issue a Privacy Notice to the Data Subject to capture the Explicit Consent.

You will need to evidence Consent captured and keep records of all Consents so that we can demonstrate compliance with Consent requirements.

Individual rights
Mind in Camden will uphold the legal rights under GDPR of people in relation to the processing of their personal data i.e. the right to:

- Withdraw consent to processing at any time
- Be informed
- Have access to their information
- Rectification of inaccurate or missing data
- Prevent our use of Personal Data for direct marketing purposes
- Erasure
- Restrict processing
- Data portability
- Raise an objection
- Rights in relation to automated decision making and profiling
- Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else
- Be notified of a Personal Data breach which is likely to result in a high risk to their rights and freedoms
- Make a complaint to the supervisory authority

You must verify the identity of an individual requesting data under 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 the Resources Director.

Sharing Personal Data
Generally, we are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee**,** agent or representative of our group (which includes our subsidiaries and our ultimate holding company along with its subsidiaries) if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers, if

- They have a need to know the information for the purposes of providing the contracted services;
- Sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's consent has been obtained;
- The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- The transfer complies with any applicable cross-border transfer restrictions; and
- A fully executed written contract that contains legally compliant third party processor/controller clauses has been obtained.

Employee responsibilities
No-one should disclose personal data outside Mind in Camden's procedures, or use others' personal data for their own purposes. This would be a disciplinary offence and possibly a criminal offence.

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our 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). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of Personal Data. You are responsible for protecting the Personal Data we hold. You must 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. You must exercise particular care in protecting Special Categories of Personal Data and Criminal Convictions Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place as requested.

Making a complaint about Data Protection
If anyone wishes to make a complaint about a data protection matter at Mind in Camden, they should contact the Chief Executive, Brian Dawn: bdawn@mindincamden.org.uk or 020 7911 0822.

People may also make a complaint about Mind in Camden to the Information Commissioner's Office.

www.ico.org.uk has detailed web pages on GDPR

Mind in Camden data protection procedures

Collecting Personal Data
Whenever we collect personal data we need to make sure that the person 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. These are described in the Privacy Policy (Appendix 1).

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. You must tell your manager immediately if these occur. Any breaches must be recorded on our Internal Breaches Register.

Documentation
GDPR requires us to document our processing activities, including 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

Sharing Personal Data
A great deal of care needs to be taken in considering whether to share data with a third party or even within different teams at Mind in Camden. Consider the risks: could anyone be damaged by it? Is the person likely to object? Might it undermine individuals' trust in the organisation that keeps records about them?

- You must have a clear reason for doing so and document what this is i.e. decide what basis. 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. You don't need to share everything you know about a person
- Sharing should be based on "need to know"
- Make sure the method of transferring the information is secure

There will need to be a separate sharing agreement with every third party with whom we share data.

Please see Sharing Personal Data (a separate document)

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 attached at Appendix 2. Managers are responsible for ensuring that records are checked

regularly and Management Team will ensure that audits are carried out as required.

Responsibility for Personal Data Management
Responsibility 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 help mainly falls within the remit of the Resources Director who is supported by staff and volunteers.

Job recruitment: job applicants will only be asked to supply information that is relevant to the role and sufficient to enable shortlisting decisions. Recruitment panels will follow the guidance in the Recruitment and Selection Policy to ensure that there is 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:
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 concerned, but in most circumstances managers will do so. Managers must follow Mind in Camden's policy on providing references.

References supplied to Mind in Camden: an employee does not necessarily have access to reference provided 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.

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.

Responsibility within the management structure:

- The Resources Director is responsible for ensuring that personnel files, including recruitment information, are kept confidential and are disposed of securely

- Sickness absence notifications are kept separately from personnel files by the Resources Director
- Supervision notes are kept by line managers.
- Payroll and pension information is kept by the Finance Department.

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

Data Security
Every Processor of personal information is responsible for dealing with it in a secure and confidential manner. 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.

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.

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.

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
- Supervision & Appraisal
- Union Recognition agreement
- Whistleblowing

Appendix 1 – Privacy policy

PRIVACY POLICY

This policy describes why we hold personal information about you and what you can expect from us in terms of managing it safely. The General Data Protection Regulation (GDPR), effective from 25 May 2018, provides you with rights and protections in relation to the use of your personal information.

Mind in Camden is the data controller of your information (as described below). You should speak to us if you have any questions or concerns. Our named person is the Chief Executive, Brian Dawn. To get in touch you can:

- Send an email to: bdawn@mindincamden.org.uk
- Phone:020 7911 0822
- Write to us: Mind in Camden, 9-15 Camden Road, London NW1 9LQ

Your personal data

Personal data includes any information which we hold now or at any time in the future which is provided to enable us either to provide service for you or to provide opportunities for volunteering or applying for job vacancies. Usually, you will have provided us with your personal information, although sometimes it may come from another organisation or person. This may include:

- Identity information (which includes: first name, middle name, last name, previous name, user name or similar identifier, title, marital status, date of birth, gender)
- Contact information (which includes: home address, address, email address, telephone numbers)
- Financial data (which includes bank account details)
- Transaction data (including details about payments made by you or for you)
- Details you have provided about yourself in relation to the service you hope to receive
- Details provided by contacts from other organisations such as your GP, support worker, care co-ordinator or referrer that are relevant to the services you use here
- Information to enable us to process applications from prospective volunteers, students, job seekers and sessional workers
- Communications data (your preferences for receiving information about our services)
- Profile data (for example, information you might provide in response to a survey, your interests, services you have used)
- Technical data (for example, analytical information about the usage of our website)

The legal position

We must have a legal reason for holding information about you (called a legal basis) and there are different legal bases that depend upon the nature of our relationship to you. For example, it will be different for someone applying to join

a group than for someone applying for a job. You will be told which legal basis applies to your personal information when you contact us.

How do we collect your information?
We collect information when you contact us by phone, email, in writing, in person, or via our websites. Sometimes, information comes to us from another organisation or person, for example, a referral. You will always be told what information we hold and how we shall use it.

How do we use your Information?
We will use your information to:

- Provide emotional support and practical help to you through our services
- Keep in touch with you e.g. about appointments, new programmes or training courses
- Help us to meet our legal obligations in relation to health and safety and equal opportunities

We will not collect any more information than is necessary to help us fulfill our responsibilities.

We will not disclose your information outside Mind in Camden <u>EXCEPT</u>:

- To health professionals if we have serious concerns regarding your immediate health and safety or the health and safety of others
- To legal and professional advisers
- To any merger or successor organisation
- To third parties not listed above where you have given your explicit consent for us to do so; or
- In circumstances where we are required or permitted to do so by law:
  - Service providers acting as processors within the UK who provide specific services
  - Professional advisers acting as processors or joint controllers including lawyers, auditors, pension advisors, bankers, insurers based in the UK who provide legal, financial, banking and insurance services
  - HM Revenue & Customs, regulators and other authorities acting as processors or joint controllers based in the UK who require reporting of processing activities in certain circumstances
  - Law enforcement and safeguarding agencies such as the Police and Camden Safeguarding Agencies

We will tell you about any information that we intend to share.

Looking after your information
Your information will be kept securely in paper form and/or electronically on our IT system. If you leave the service, your information will be kept in an archive until it is securely destroyed after a certain length of time. The length of time that we keep information varies depending on what kind of information it is. There are legal requirements about keeping certain types of information for a set period of time but, in other cases, it is a matter of what is good practice.

What rights do you have?
GDPR gives you certain rights over your information, which are:

- The right to be informed: you should know what information we have and how we will use it
- A right of rectification: the information we keep about you should be accurate and up to date information. If any of your details are missing or incorrect, please let us know and we will put it right and, with your consent, pass on the correct details to any other organisation that we are working with on your behalf
- The right to erasure: you have the right to have personal information erased (it is also known as "the right to be forgotten") under certain circumstances, for example, if we were holding the information unlawfully. However, it does not apply where we have a legitimate interest in keeping it or a legal obligation.
- The right to restrict processing: this also applies under certain circumstances and it would usually be for a time limited period. For example, if you thought the information we held about you was wrong you could ask for us not to use the information until the matter had been investigated.
- The right to data portability: you can obtain a copy of your personal information if you wanted to pass it to another organisation, or ask us to send it to another organisation if it is technically feasible to do so.
- The right to object: you can object to your information being used for direct marketing purposes or for being used for scientific or historical research. You can also object to us using your information where we are relying on a legitimate interest for doing so and you have grounds relating to your particular situation.
- The right not to be subject to the decisions made by automated processing or profiling which has legal effects that significantly affect you. Automated processing is when decisions are made without any human involvement. At present, this is not something with which Mind in Camden engages.
- Right to withdraw your consent to any processing where we have used consent as our legal basis to process your personal information

If you wish to take up any of these rights, you will need to inform us, ideally in writing. To protect your privacy and the security of your information, we may take reasonable steps to verify your identity before we act on any request that you may make in respect of your Information. We will respond within 30 days wherever possible (but will let you know in writing if there is a reason for it taking longer and when you can expect a response). Please note that some of these rights apply only in certain circumstances.

Complaints about your personal information
If you wish to make a complaint about any aspect of the way we treat your information, you can contact Brian Dawn, Chief Executive on 020 7911 0822 or bdawn@mindincamden.org.uk or in writing to: Mind in Camden, 9-15 Camden Road, London NW1 9LQ. Alternatively, you can also make a complaint to the Information Commissioner's Office www.ico.org.uk

Please note: this is only for making a complaint about the way your personal information is being collected or used. If you have any other complaint about our services please use our Complaints Procedure – you can ask any member of staff for a copy of this procedure.

Appendix 2 – Retention of documents

Record	Length of time to be kept	Reason
Employment records		
Accident books & records	3 years after the last entry	RIDDOR 1995
Accounting records	6 years	Companies Act 1985
Income tax & NI returns & correspondence with the Inland Revenue	3 years after the end of the last financial year to which they relate	Income Tax (Employments) Regulations 1993
SMP & SSP records	3 years after the end of the last tax year to which they relate	SMP (General) regulations 1982 & SSP (General) regulations 1982
Salary records	6 years	Taxes Management Act 1970
Medical records specified by COSHH regulations	40 years from the date of the last entry	COSHH regulations 1999
Records of tests carried out under COSHH	5 years from the date on which they were carried out	COSHH regulations 1999
Recruitment – application forms & notes from interviews	1 year	Recommended period (CIPD)
Personnel files	6 years after employment ceases	Recommended period (CIPD)
Redundancy details	6 years from the date of redundancy	Recommended period (CIPD)
Trade Union Agreements	10 years after ceasing to be effective	Recommended period (CIPD)
Management Committee deeds, rules & minute books	Permanently	Recommended period (CIPD)
Assessments under H&S regulations	Permanently	Recommended period (CIPD)
Tender documents – successful & unsuccessful bids	6 years	Recommended (dti)
Incorporation documents		
Incorporation Documents		
Certificate of Incorporation	Permanently	Companies Act 1985

Certificate of change of company name	Permanently	Companies Act 1985
Memorandum & articles of association (original)	Permanently	
Memorandum & articles of association (current)	Permanently	
Printed copy of resolutions filed at Companies House	Permanently	Resolutions must be minuted & included in the Memorandum & Articles of Association
Meetings		
Notices of general & class meetings (signed copy)	Permanently	
Circulars to shareholders (master copy)	Permanently	
Board minutes (signed copy)	Permanently	
Board committee minutes	Permanently	
Written resolutions of the Board	Permanently	
Minutes of general & class meetings	Permanently	
Statutory written resolutions of company	Permanently	
Statutory returns, records and registers		
Annual return excluding list of members (1 copy)	Permanently	
Directors' service contracts	6 years after cessation	
Register of directors & secretaries (original)	Permanently	
Register of documents sealed	Permanently	
Accounting and tax records		
Accounting records to comply with CA, s.221	Ltd – 3 years	
Signed copy of report & accounts	Permanently	
Interim report & accounts	Permanently	
Budgets & periodic internal financial reports	2 years	
Tax returns and records	10 years	

VAT records	6 years.	
Banking records, including Giro		
Cheques, bills of exchange & other negotiable instruments	6 years	
Paying-in counterfoils	6 years	
Bank statements & reconciliations	6 years	
Instructions to banks	6 years after ceasing to be effective	
Charitable & political donations		
Deeds of covenant (done)	12 years after last payment	
Documents evidencing entries in accounts re donations	6 years	
Contractual & trust agreements		
Contracts under seal	12 years after expiry	
Other contracts	6 years after expiry	
Trust deeds (original & copy)	Permanently	
Inland Revenue approved and statutory pension schemes		
Accounts & supporting documents	Accounts, permanently	
Property Documents		
Leases	12 years from termination and any terminal queries (e.g. dilapidations) have been settled	