mind in the City, Hackney and Waltham Forest

DATA PROTECTION POLICY

---

1. Introduction

Data Protection legislation such as the Data Protection Act (2018) and the General Data Protection Regulations (GDPR) regulates the collection, storage, use and disclosure (processing) of personal data about identifiable living individuals by organisations. Any organisation that keeps personal information about living individuals must comply with the Act.

Personal data is any information about a living individual which makes them uniquely identifiable. It applies to service users, staff, donors and volunteers. The information may be stored on computer (including websites) or other electronic equipment with automatic retrieval or in a relevant filing system (a paper-based record keeping system structured in such a way that information about a particular individual can be readily located). It can include video, CCTV, photographs, and other non-text data.

Everyone in Mind in the City, Hackney and Waltham Forest (Mind CHWF) has their responsibility to manage, use and where appropriate, share this personal data in a secure and confidential way.

The member of staff responsible for Mind CHWF's management of data protection is the Information Governance Lead.

2. Policy Statement

This policy focuses on personal data and is intended to interpret the Data Protection Act (2018). It supports Mind CHWF's values to treat everyone fairly and with respect and to be honest and professional in the way we deal with people.

This policy applies to all Mind CHWF staff and volunteers including sessional staff and contractors, working at all sites and locations. Individuals need to be aware of their responsibilities, and that a breach of security or infringement of confidentiality could lead to disciplinary action and even prosecution.

For more information about confidentiality and security please refer to MIND CHWF's Confidentiality Policy and staff handbook.

3. Key Points

Key points for staff, volunteers, and contractors to follow are:

We are required to inform anyone whose personal data we process about how their information may be used;

• Personal data should always be kept secure and confidential; controls are put in place to ensure that staff, volunteers and contractors only have access to the personal data that is necessary for them to do their job;

• Individuals have the right to see what personal information is held about them, and to request that any errors are corrected. This request must be recorded although the organisation may have a reason why the change should not be made;

• Any disclosure of personal data must comply with the Data Protection Act (2018);

• When personal data is shared it should be kept anonymous wherever and whenever possible;

• Common sense precautions for protecting personal data include: not divulging computer passwords, keeping manual records secure and guarding against people seeking information by deception.

Mind CHWF's staff, volunteers and contractors must notify the Information Governance Lead of any relevant filing systems or computer databases that contain (or will contain) personal data (e.g. name and address) so that it can be accounted for in Mind CHWF's Information Governance Toolkit submission and our Record of

Processing Activities.

4. Compliance with the principles of the Data Protection Act (2018)

Two key components of maintaining confidentiality are the integrity of information and its security. Integrity is achieved by safeguarding the accuracy and completeness of information through proper processing methods. Security measures are needed to protect information from a wide variety of threats. These components are underpinned by the seven 'principles' of the Data Protection Act (2018).

Failure to comply with the principles of the Data Protection Act could mean that a criminal offence has been committed, in which case you may be liable to criminal prosecution individually.

Data Protection Principles as set out in the Data Protection Act 2018

First Principle of the Data Protection Act

The first principle states that personal data shall be processed fairly, lawfully and in a transparent manner.

The general interpretation of this principle is that data subjects (service users, staff, etc.) should be fully informed about how their information may be used and the extent to which it may be shared. In some circumstance data subjects may have to be asked for their express consent for processing and sharing to take place and have the opportunity to make known any objections.

If an individual (having been fully informed about the use of their information, including about the consequences, and having had the opportunity to object) wants information

about them to be withheld from a third party, the individual's wishes should be recorded and, whenever feasible, respected (see separate procedures).

All individuals whose personal data is collected and stored should have access to a copy of MIND CHWF's privacy policy in order to ensure that they are fully informed about how their information may be used and the extent to which it may be shared.

Second and Third Principles of the Data Protection Act

The second and third principles state that personal data shall be obtained for specified, explicit and legitimate purposes and not be processed in a manner that is incompatible with those purposes. Data obtained shall be adequate, relevant and limited to what is necessary.

Taking these principles together, Mind CHWF's staff must ensure that there is clarity about the purposes for which personal data is collected and used, that only the minimum personal-identifiable information necessary to satisfy those purposes will be collected, and that the information is used only for those purposes. Individuals must be informed about the purposes for collecting data and their consent must be obtained if the data is used for any purposes beyond the original purpose, except for where the data is used to comply with any other lawful purpose.

Any Mind CHWF's staff, volunteers and contractors who are unclear whether the data they are collecting complies with these principles should contact the records manager for guidance.

Fourth Principle of the Data Protection Act

The fourth principle states that personal data shall be accurate and kept up to date.

All Mind CHWF's staff, volunteers and contractors must ensure that all personal data for which they are responsible is accurate and up to date. If staff discover that personal data is incorrect or misleading, they must take reasonable steps to correct or erase the data as soon as possible, this should be actioned with guidance from the information governance lead.

Mind CHWF staff, volunteers and contractors must also be aware and support individuals' rights to rectify incorrect personal data. Please see below for further details on this as part of the subject access request process.

Fifth Principle of the Data Protection Act

The fifth principle states that personal data shall not be kept for longer than is necessary.

All Mind CHWF's staff, volunteers and contractors must ensure that the personal data for which they are responsible is not kept for any longer than is necessary.

In order to guide staff on how long information should be kept, MIND CHWF's Data Retention and Disposal Policy sets out the retention periods for the different types of

information and the procedures for its safe and secure disposal.

Any Mind CHWF's staff, volunteers and contractors who are unclear how long they need to keep the personal data for which they are responsible should contact the Data Protection Officer for guidance.

Sixth Principle of the Data Protection Act

The sixth principle states that personal data shall be processed in a manner that ensures appropriate security of personal data including, protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures.

Mind CHWF has taken the appropriate organisational and technical measures to ensure that data is stored and processed securely.

All Mind CHWF's staff, volunteers and contractors are responsible for ensuring that the personal data for which they are responsible is kept securely and is not accessible by anyone who does not need to have access.

Seventh Principle of the Data Protection Act

The seventh principle of the 2018 Act is accountability. This makes the organisation responsible for maintaining compliance with the Act and the principles above and to be able to demonstrate this compliance.

This policy forms part of our demonstration of compliance and works in conjunction with other policies named throughout this policy.

The organisation also maintains a variety of records that relate to data protection: Records of Processing Activities, log data breaches and near misses, log of subject access requests, log of internal spot checks relating to information security, Privacy Impact Assessments as part of all project implementation documents and written contracts of data processing with sub-contracted organisations.

Mind CHWF staff, volunteers and contractors also all receive mandatory training on data protection and along with other processes these are reviewed annually or when there are substantial changes which may impact data protection (these may be internal or external, such as changes to IT infrastructure, moving premises or updates in technology that offer opportunities to increase data security).

5. Confidentiality

Mind CHWF takes its obligations to maintain the confidentiality of personal data very seriously. All Mind CHWF's employees, contractors and volunteers should recognise each individual's right to confidentiality in order to meet legal requirements and retain the trust of data subjects. Further information on confidentiality can be found in Mind CHWFs Confidentiality and Access to Records Policy.

Confidentiality is between an individual and Mind CHWF as an organisation and not between an individual and a member of staff. All personal information must be treated in the utmost confidence and not divulged to anyone outside the organisation except where extenuating circumstances exist. However, in order that we can provide the best possible help to our service users, it may be necessary to share information with other services or managers within Mind CHWF or external organisations.

All staff that have access to personal data are responsible for taking the necessary steps to safeguarding its confidentiality.

Even when consent to disclose has been obtained, personal data must still be used only in ways that safeguard the confidentiality of the personal data (including appropriate anonymity whenever and wherever possible).

Individuals who do not have a contract with Mind CHWF (and are not covered by an agreement or contract), but are working on behalf of Mind CHWF will be required to sign Mind CHWF 's Personal Data Processing by Third Parties Agreement.

Where a contract is placed with another organisation for services which involve sharing or disclosure of personal data, the parties concerned must also sign the agreement.

Any employee or volunteer with any concerns regarding information kept by Mind CHWF should consult Mind CHWF's confidentiality policy, staff handbook or raise it with their line manager or Mind CHWF's Information Governance Lead.

5.1 The Recording of Telephone Calls

The recording of telephone calls is governed by a number of different pieces of UK legislation. If recording calls, callers should be made aware that the recording is taking place. Individual staff are not permitted, under any circumstances, to record any telephone calls made to, or received by, Mind CHWF. This includes all calls made and received on a fixed line and mobile telephones and all internal calls. Members of staff found to have recorded conversations may be subject to disciplinary procedures and/or subject to criminal prosecution.

6. Special Category Data

Further requirements apply to the processing of data defined as 'special category personal data'. Special category personal data is defined by the Data Protection Act as personal data relating to an individual's:

- Race;
- Ethnic origin;
- Religion;
- Politics;
- Trade union membership;

• Genetics;

• Biometrics;

• Health;

• Sex life;

• Sexual Orientation.

The threshold for use of confidential and special category personal data is higher than for the use of other forms of information because unnecessary or inappropriate use of this sort of information is likely to cause damage, distress or embarrassment to individuals. As a consequence, best practice dictates that access is restricted on a strictly 'need to know' basis.

7. Subject Access Requests

7.1 Definition

The Data Protection Act (2018) gives all individuals, or Data Subjects, the right to know what information Mind CHWF holds about them. This includes all the people who currently use our services or have used them in the past, donors, volunteers and staff.

A request from a Data Subject to see what information we hold about them is called a Subject Access Request.

All Subject Access Requests can be made verbally or in writing . All requests must include some form of proof of identity, such as a copy of a birth certification, driving license, etc. before it can be acted upon. The identification provided should be verified against the record that we hold of the person which should include a unique identifier such as full name and date of birth. If a request does not contain any form of proof of identity, this must be requested before any further action can be taken.

In general, no fee will be charged for responding to a Subject Access Request. Exceptions to this are when the organisation deems the request to be manifestly unfounded or excessive or if the individual requests further copies of their data following their initial request being responded to. This fee will be of a reasonable amount and associated with the administrative cost of complying with the request. Data subjects must provide sufficient information to allow the personal data they are seeking to be located if there is specific data looking to be identified. If there is insufficient information to locate the data or if the request is too broad in its scope, the data subject may be asked to provide further information to allow the request to be met. Alternatively, the data subject can request all data that Mind CHWF holds.

E-mails fall within the scope of the Data Protection Act. Data subjects must supply enough information to enable Mind CHWF to locate the relevant emails, such as:

• The fact that the data may be held in the form of emails;

• The names of the authors or recipients of the messages;

• The dates or ranges of dates upon which the messages have been sent;

• Any other information that might assist Mind CHWF in locating the data.

Failure to provide information reasonably required to narrow down the search could result in Mind CHWF requesting further information to be able to comply with a Subject Access Request.

Once we are satisfied that the Subject Access Request is valid, the applicant has provided proof of identity and we are satisfied that the request is satisfactorily defined we have one calendar month in which to respond, with the possibility of extension for up to 2 months for complex requests (we will inform individuals within the calendar month if and for what reason we need to extend the time limit). The one-month timeframe starts when all these conditions have been met.

7.2 Who may seek access?

Any individual is entitled to see their own information. However, they may only have access to information about themselves. They are not entitled to see information about any other individual without consent.

In certain circumstances it may be possible for someone other than the data subject to access personal data. This includes: an individual with parental responsibility; a solicitor or similar agent appointed by a service user with capacity; a child's Guardian appointed by the court; or an agent appointed by someone with parental responsibility. This is dependent on a letter of authority and a copy of identification from the solicitors.

7.3 Access to Personal Data

During the course of their normal business the following Mind CHWF's staff and volunteers may be permitted to access service user personal data:

• Any member of staff or volunteer who is directly responsible for working with personal data in order to carry out their job;

• Line managers who need to access files that their staff are working on;

• Members of staff or volunteers who receive permission from the appropriate manager or director;

• The records Manager for the purpose of auditing records, management of policies and procedures and archiving.

• Anyone with the relevant authorisation; such as an external inspection agency or an internal auditor.

7.4 Exemptions

Mind CHWF retains the right to refuse access in certain circumstances. These are known as exemptions. The decision to refuse access is a significant one and therefore must be taken in conjunction with the Information Governance Lead and agreed with

management before informing the data subject, all exemptions should be reviewed on a case-by-case basis and cannot be applied as a blanket policy.

Mind CHWF can refuse to comply with requests that are manifestly founded or excessive. The decision of whether a request falls under either of these reasons will be made by the Information Governance Lead on a case-by-case basis.

7.5 Dealing with Subject Access Requests

It is the responsibility of individual managers and team who collect, store and use personal data to respond to requests for access. It is important therefore that staff and volunteers are aware of the provisions of the Data Protection Act (2108), Mind CHWF's Data Protection policy and the importance of keeping records up to date and accurate. However, because of the complexity of the Act, specialist advice from the Information Governance Lead must be sought to ensure that the Act is applied correctly.

Mind CHWF's Information Governance Lead must be notified of all subject access requests, including the outcome, for monitoring and reporting purposes.

Records containing personal data may be found in many places, including: case files, e-mails, personal and shared electronic folders and databases. All of the places where information is stored must be searched for any personal data falling within the scope of the request, providing the scope has been adequately defined (see above).

Any member of staff or volunteer who it is felt may hold, or have access to, personal data which falls within the scope of the request must be contacted and the relevant data provided to the person dealing with the request. This includes any relevant emails which are stored in Outlook and Teams folders or on Sharepoint.

Once gathered, the designated member of staff or volunteer must review all of the information with the Information Governance Lead in order to decide what information falls within the scope of the request and may therefore be released to the subject. As part of this process, if there are any references to identifiable third parties a decision nmust be made as to whether or not to disclose this information. The information governance lead should make attempts to gain the consent of the individual and if they are unable to do so needs to decide whether or not to redact the information when the data is given to the individual who requested it.

Once a request has been received, only routine amendment that would have been carried out anyway may be made to the relevant file. No records that fall within the scope of the request may be removed or deleted from the file, inbox or electronic drive.

Data subjects may choose how they would like to view their information. However, the Act contains a duty of care which means that every effort must be made to avoid causing distress or suffering as a consequence of seeing the personal data. In cases where it is felt that the material being accessed may cause distress, the data subject should be invited to view the data in the most convenient Mind CHWF office so that the data may be explained. The data subject should also be offered any necessary help and

support such as counselling or the support of a social worker. The data subject may be accompanied by a friend, relative, or advocate if they wish.

If the data subject does not wish a Mind CHWF member of staff or volunteer to be present when viewing their data, this should be respected wherever possible. However, any decision must take into account the possibility of distress that the data may cause the data subject.

In some cases, such as when an individual refuses the offer of support or with data relating to donors, volunteers and staff, the use of a social worker will not be appropriate. In this case the data may be disclosed by copying the relevant records and sending them to the data subject (ensuring that any exempt information is blanked out). However, any decision not to take up Mind CHWF's offer of support must be recorded and the data that is being sent to the data subject must be checked and agreed with the information governance lead and management. A copy of the response must be recorded.

1Records should not be removed from the office except with the consent of the relevant line manager or Mind CHWF's Information Governance Lead.

Wherever possible, the data being provided to the data subject must also be copied and put on record along with the covering letter and proof of identity. Where it is not practical to copy and file all of the data provided in response to a subject access request, the relevant records should be indicated either by marking or by listing them.

The Data Protection Act gives data subjects the right to amend information which they feel is incorrect. If the data subject wishes to amend the records in any way the change must be agreed with line management. If it is decided that the record should not be changed, a note will be made of the request and the data subject informed.

The process for dealing with subject access requests is illustrated with a process map at the end of this document.

7.6 Providing Information as part of Police Investigations

Occasionally Mind CHWF is asked to provide access to its files as part of a Police Investigation. All such requests must be passed to MIND CHWF's Information Governance Lead and Caldicott Guardian to deal with.

Access to Mind CHWF's files for the purpose of a Police investigation will only be granted if accompanied by a Court Order or the consent of the data subject. Requests should be received in writing and signed off by the Information Governance Lead or a similarly senior officer.

7.7 Right to Appeal

Anyone who is refused access to their personal data may appeal against the decision via our Complaints, Compliments and Feedback Process. At this point individuals should be made aware of their right to refer directly to the Information Commissioners

Office, alternatively they may do this once they have received a decision through our Complaints Process.

Please refer to our Complaints Policy for further details on this process.

8. Information Security

The increasing reliance on technology for the provision of MIND CHWF's services makes it necessary to ensure that systems are developed, operated, and maintained to promote and secure an appropriate level of protection and confidentiality.

All members of staff, volunteers and contractors who use or have access to personal data via these systems are responsible for ensuring that this information is kept securely and is not passed to anyone outside of the organisation without permission.

Staff should be aware of the IT policy which includes the standards the organisation holds for password security and how to access records appropriately from approved devices. The Confidentiality and Access to Records Policy is also vital in maintaining the security of physical records of data and should be read in conjunction with this policy.

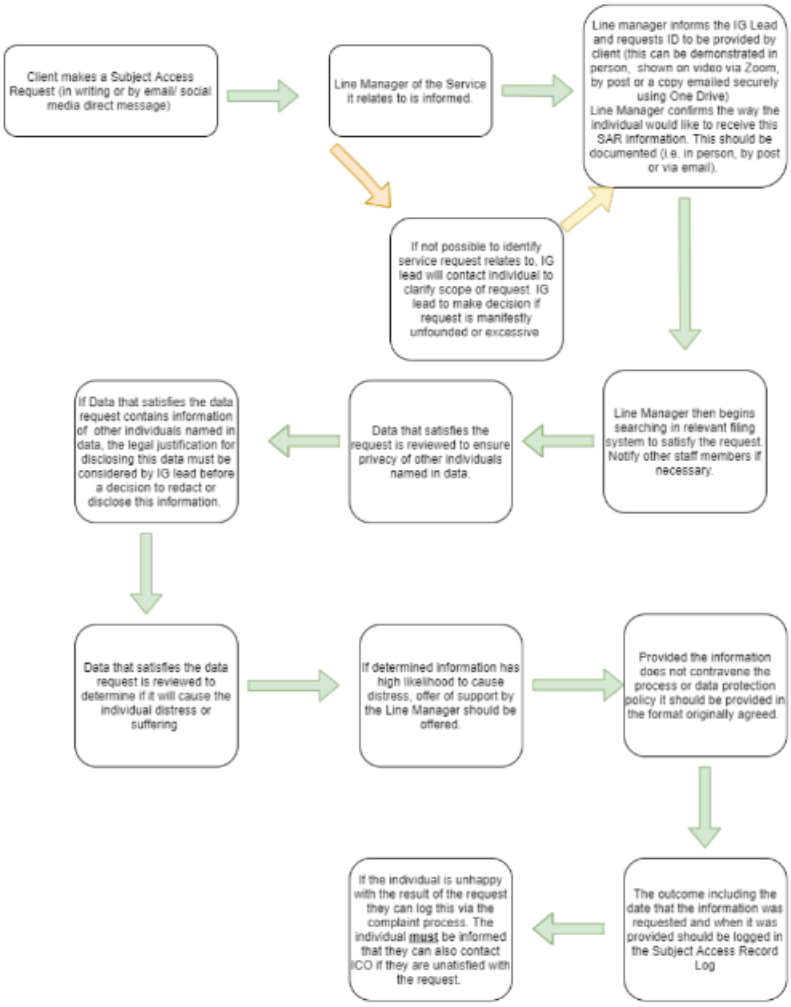
Any third-party organisation that processes data on our behalf must have adequate data protection measures in place. Mind CHWF will undertake a due diligence exercise before engaging any such third party and they must sign a Personal Data Processing by Third Parties Agreement as a written guarantee that they comply with the principles of the data protection legislation.

9. Personal Data Breaches

Whilst Mind CHWF will take all the necessary measures to ensure that personal data is processed securely there may be instances where the security of this data is breached. Whether through human error, technical error or attacks from malicious individuals trying to access this data Mind CHWF will ensure that the required steps are taken to inform individuals and the relevant authorities. Staff should refer to the Data Breach Policy if they suspect a data breach has occurred or if there is a near miss where a data breach may have occurred.

APPENDIX

Subject Access Request Process Map (next page)



Policy	Data Protection
Policy Type	IT and IG
Policy Number	CHWF DP22 v4
Date Approved	March 2024
Date of Next Review	January 2026