mind Coventry and Warwickshire

Data Protection Policy

Contents

1. Definitions

a. Data

Any information about a personally identifiable individual that we hold. CW Mind will specify the legal basis for processing each type of data. Certain data is specified as 'special category' and needs extra justification for processing.

b. Processing

Any of the following actions: obtaining, accessing, recording, retrieval, consultation, holding, disclosing, sharing, using, transmission, erasure, destruction.

c. Data subject

Data subject means an individual who is the subject of the personal data, either directly or can be identified from it. A data subject must be a living individual.

d. Data Controller

The Data Controller is the individual, company or organisation that determines the purpose and the manner in which personal data may be processed. CW Mind is the Data Controller for the purposes of the General Data Protection Regulation.

e. Data Processor

Data Processor, in relation to personal data, means any other person other than an employee of CW Mind who processes the data on behalf of CW Mind.

f. Recipient

Recipient, in relation to personal data, means any person to whom data are disclosed (including employees or agents of CW Mind).

g. Third Party

Third Party means anyone other than the data subject, the data controller or any person authorised to process data on behalf of the data controller.

h. Data Protection Legislation

Within this policy, 'data protection legislation' means the General Data Protection Regulation (GDPR), the Data Protection Act 2018, or any subsequent UK data protection legislation.

2. Commitment

This policy outlines how Coventry and Warwickshire Mind collects, uses, stores and protects data and information about the people who interact with our services (including service users, volunteers, trustees and staff).
CW Mind adheres to the principles of UK GDPR Legislation.

Article 5 of the UK GDPR requires that personal data shall be:

“a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) 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, using appropriate technical or organisational measures."

Article 5(2) requires that:

"the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

CW Mind has in place processes and procedures to ensure that these principles are upheld across our data processing activities.

3. Purpose

The purpose of this policy is to protect the rights and privacy of living individuals who access CW Mind services, work for, or support CW Mind, to ensure that personal data is not used, stored or disclosed ('processed') without such individual's knowledge, and is processed with a lawful basis and in a fair and transparent manner.
We will abide by the seven key principle as set out by UK GDPR legislation.

Article 5(1) requires that personal data shall be:

Lawfulness & Fairness: Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.

Purpose Limitation: Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Data Minimisation: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy: Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

Integrity and confidentiality (security): Personal data shall be processed in a manner that ensures security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical or organisational measures.

Accountability: The accountability principle requires that we take responsibility for what we do with personal data and how we comply with the other principles.

Appropriate measures and records will be kept to be able to demonstrate compliance.

In simple terms, this means we must collect and use personal data fairly, tell people how we will use their personal data, store it safely and securely and not disclose it unlawfully to third parties. We need to be careful that the information we collect is relevant and that we do not collect more information than we need for the stated purpose.

There are restrictions on the transfer of personal data outside the EEA and information should not be transferred outside of the UK unless it meets the requirements of the Data Protection Legislation.

Partners and any third parties working with or for the organisation, and who have or may have access to personal data, will be expected to comply with the principles of this policy. No third party may access personal data held by the organisation in a routine way, without having first entered into a third party Data Sharing Agreement which imposes on the third party obligations no less onerous than those to which the organisation is committed, and which gives the organisation the right to audit compliance with the agreement.

4. Duties & Responsibilities

a. Chief Executive

The Chief Executive has overall responsibility for Information Governance which includes data protection legislation. As the accounting officer he/she is responsible for the management of the organisation and for ensuring mechanisms are in place to support service delivery and continuity.

b. Chair

The Chair has Board level responsibility for the management of information risk within the organisation and the development and maintenance of Information Governance practices throughout the organisation, including business continuity measures to ensure the safety and availability of information assets.

c. The Board of Trustees

The Board is responsible for ensuring that the organisation establishes, monitors and maintains systems, processes and reporting arrangements for the management of all aspects of information governance, data protection and confidentiality. It supports and drives the broader information governance agenda and provides assurance that effective information governance best practice mechanisms are in place throughout the organisation.

d. IG Manager

Responsible for the operational day to day management of all issues relating to information governance, data protection and confidentiality, including drafting policy documents, procedural guidance, training, audit and dealing with all information governance related enquiries.

e. Managers

Managers are responsible for ensuring that there are procedures in place relevant to their area of work, that their team are familiar with and follow those procedures, and that their team complete GDPR refresher training annually.

f. All Staff

It is the responsibility of all staff at CW Mind to:

i. familiarise themselves with and follow the policies/procedures in place relevant to their role or work.
ii. be responsible for the safety and proper management of the information they process, and for the prompt reporting of any information governance incidents using Data Breach Reporting Form (QU24) following PRC71 – Data Breach Reporting Process. The Data Breach Reporting Form (QU24) must be shared with IG Manager for further action.
iii. complete Information Governance refresher training annually.
iv. All staff must maintain confidentiality, security and integrity of information relating to service users. The unauthorised access or disclosure of service user or other personal data is regarded as gross misconduct and will be subject to CW Minds

Disciplinary Procedure, and in the case of computerised information, could result in prosecution for an offence or action for civil damages under the Data Protection Act.

5. Lawful basis

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever CW Mind processes personal data:

- **Consent:** the individual has given clear consent for us to process their personal data for a specific purpose.

- **Contract:** the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

- **Legal obligation:** the processing is necessary for us to comply with the law (not including contractual obligations).

- **Vital interests:** the processing is necessary to protect someone's life.

- **Public task:** the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

- **Legitimate interests:** the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

- **Special Category Data**: Special category data is personal data which the GDPR says is more sensitive, and so needs more protection. This means if CW Mind wishes to process the following data, the organisation will need to also obtain specific consent from the data subject:

    - Race or ethnicity
    - Political, religious or philosophical beliefs
    - Trade union membership
    - Genetic data and biometric data (where used for ID purposes)
    - Health
    - Sexual orientation or details concerning a person's sex life

- **Criminal Offence Data:** CW Mind will comply with any conditions under Data Protection legislation.

CW Mind uses a different legal basis for different services provided, dependent on the types of information we need to process. Please see Data Kept, below.

6. Data kept

CW Mind will keep an ongoing log of the data we keep, our lawful basis for keeping it, where and how it is used, where and how it is kept and for how long. Please see **QU25 - Record of Processing Activities.**

CW Mind collects, uses and stores a range of personally identifiable data relating to service users, volunteers, trustees, staff, members and supporters. This information enables us to:

1) provide quality services that are tailored to individuals' needs;
2) demonstrate that we provide fair and open access to all our services;
3) ensure that service information is only ever shared with the person to whom it concerns;
4) share relevant news and information with individuals based on their relationship/involvement with CW Mind; and
5) better understand the need and demand for our services from different demographics.

We also store data and information relating to individuals' interactions with our services (i.e. case notes) as well as the nature of their support needs (including medication requirements as necessary). This ensures that:

1) we are accountable for the support that we provide;
2) we provide services that are based on an individual's needs;
3) we provide a seamless service to our service users; and
4) we have evidence about our service outcomes.

Case notes (including safeguarding records) are always treated as 'sensitive data' to protect the privacy of everyone involved.

Depending on the service provided, we may also collect and store some of the following information:

- Referral information from third parties (*this should only have been shared with us with the service users consent)
- GP details
- Next of kin contact details
- Information about other third-party services being accessed

This ensures that, when required, we can liaise with referrers, GPs and people from within an individual's support network to ensure that they receive the best quality care and that they remain safe and well at all times. However, this information will only be used with the consent of the service user and/or if there is a statutory obligation to do so (see more information under 'breaches of confidentiality' below). As and when sharing information of this nature is felt to be a likely/necessary part of someone's support needs within a particular service, formal

consent will be sought from the service user at the beginning of their interaction with the service.

At regular intervals, we collect feedback from our service users via online surveys and questionnaires. These are anonymous by default; however some service users choose to give us their details, in which case this data is treated as sensitive data. In some cases, we also collect case studies to demonstrate the impact of our services and/or to publicise fundraising activity, however individuals are always given the option of remaining anonymous.

At times, we may also collect contact information from individuals if they would like to receive news and information relating to CW Mind - however individuals have the opportunity to unsubscribe from unwanted emails at any time.

Location of data:

Exchange: European Union
SharePoint: United Kingdom
Skype: European Union
Teams: European Union
Charitylog: United Kingdom

7. Transportation of data

Wherever possible, personal information will not be transported on paper.

Precautions will be taken when transporting personal information, both within and outside the organisation, to ensure that it is protected from unauthorised access, loss or destruction.

a. Paper files

Where it is necessary to transport documents or files relating to staff, volunteers, trustees or service users, the employee with the responsibility for transportation will ensure that no personal information is visible, i.e. in a non-transparent container.

Wherever possible documents will not be taken home overnight; where it is not possible to return paperwork to an office by the end of shift, the employee is responsible for the confidentiality of the document/s and so should ensure that they keep the data in a secure building during this time (i.e. NEVER left in a car). Should confidentiality be broken the protection of information is the responsibility of the member of staff who is in possession of the information. Failure to take adequate measures to protect information may lead to disciplinary and/or legal action being taken against the individual.

b. Removable media

Staff must not store, convey or transmit identifiable and/or sensitive information in an unencrypted format on removable media/devices. This relates to all types of removable devices/media (including CD's, DVD's, Memory Cards, USB pen drives, USB hard drives). These items are small, light and potentially easily lost. They can also contain high volumes of data/information for their size. Where used, removable media must be encrypted and where sensitive data is stored on removable media, the documents must be password protected.

Staff must not connect, install and run any other software or removable media such as MP3 players, mobile phones or iPods on or with CW Mind's IT equipment. CW Mind will not bear any responsibility for such damage to equipment or loss of personal data in these cases.

CW Mind reserves the right to recall all removable items whether belonging to the organisation or personal, where it is believed that confidential data is being stored or transferred in an insecure manner, not compatible with this policy. In such an instance, this may lead to disciplinary action being taken.

c. Email

When an email is sent where the message contains personal data, the email will be encrypted. Where an email attachment contains personal data, this document will be password protected and the password relayed to the recipient in a separate email or verbally. When an email is sent to multiple service users Bcc will be used to hide the contact details of the service users from each other.

d. Portable IT Equipment

Where portable IT equipment is used (i.e. laptop, tablet, smartphone), it should be protected by a password, and the employee is responsible for the confidentiality of the data held within it and so should ensure that they keep the equipment in a secure building outside of working hours (i.e. NEVER left in a car). Should confidentiality be broken, the protection of information is the responsibility of the member of staff who is in possession of the information. Failure to take adequate measures to protect information may lead to disciplinary and/or legal action being taken against the individual.

8. Data retention & destruction

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

CW Mind will regularly:

- review the length of time we keep personal data;
- consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Please see **QU06- Data Retention Schedule** for more information.

9. Backups / Updates

In some areas of work, software backups are necessary to ensure no loss of data. Wherever this is in place, there will be a specified backup protocol for staff to follow, including checking that the backups are working correctly.

Software updates are necessary to ensure that up-to-date security measures are in place on all devices. Wherever possible, CW Mind will handle this remotely.

10. Access to files

Individuals have the right to access their personal data: this is commonly referred to as subject access or SAR or DSAR.

Individuals can make a subject access request in writing or verbally, direct to any member of staff. The member of staff receiving the request needs to clarify with the person exactly what they would like to see by completing **QU31- Subject Access Request Form**. CW Mind have one month to respond to a request.

Please also see **PR20- Subject Access Request Procedure**.

11. Freedom of Information

CW Mind undertakes to use its best endeavours to keep confidential any information provided to it, subject to the statutory obligations under law, including the Freedom of Information Act 2000.

If CW Mind considers that any information communicated to the organisation should not be disclosed because of this sensitivity then this should be stated, together with the reason for considering it sensitive. CW Mind will then use reasonable endeavours to consult with affected people in considering any request received under the Freedom of Information Act 2000 before replying to such a request. It should be noted however that CW Mind does not have discretion in responding to such request under the Act.

12. Breaches of data protection/incidents/reporting

Incidents or any near miss that affects the confidentiality, integrity or availability of information, and /or led to the unauthorised destruction, denial of access, disclosure or modification of information, is a data breach and must be reported immediately to the Information Governance Manager (if they are unavailable, contact Head Office). This will aid in improving awareness, eliminating poor practice and carelessness, rather than apportioning blame. Please see **PRC 71 – Data Breach Reporting Process** for more information.