Conwy Mind
Confidentiality Policy

Date Created: June 2019

Date Approved: July 2019

Date of Review: July 2020

Overview

Confidentiality refers to our duty not to reveal to any third party any information relating to another party, which has been given to us in trust. Under the Human Rights act 19981 the right to confidentiality (article 8 Private and Family Life*) is now covered by statute. This policy should be read, interpreted and implemented in accordance with that Act.

All staff are likely, in the course of their work to handle confidential information regarding this organisation, other organisations and individuals. Members of the Executive Committee, employees and volunteers may also have access to such information. This may be verbal or written material e.g. Telephone messages, reports, committee minutes, management and financial information. It is essential that everyone involved in the organisation respect and maintain the confidential nature of any material so classified. Conwy Mind acknowledges that process of confidentiality within an organisation is complex and recognises both individual and corporate confidentiality.

The aim of this policy is to:

- Protect service users, employees and volunteers from the possibility of information about them being passed on to individuals or organisations who have no right to that information.
- Reassure service users that care will be taken with information they give to employees and volunteers and to enable them to trust those who are providing a service to them.
- Provide guidance to employees and volunteers on the extent to which confidentiality is to be preserved, circumstances in which they may breach confidentiality, and measures to be taken for the safeguarding of information.
- Assist employees and volunteers to comply with legal and statutory requirements for the disclosure of information.
- Reassure service users wishing to make a complaint to or about Conwy Mind that the confidentiality of any complaint will be given high priority in so far as this is consistent with the need to investigate the complaint.

Fulfil obligations under the Data Protection Act (DPA) 1998.

1. Principle

All staff and volunteers have a duty to keep personal information about service users safe and confidential. Service users need to feel that they can trust staff if they are discussing personal or sensitive matters with them and every service user has a basic right to privacy.

Staff and service users have the absolute right to access information that Conwy Mind has recorded relating to them.

Staff and volunteers must not discuss service users outside of work, must not gossip about service users whilst at work, and must be mindful of whether they can be overheard by others when discussing sensitive or confidential information about service users.

Confidentiality does not mean secrecy. Current mental health care has a multi-disciplinary approach, which requires good communication and good information exchange for it to be safe and effective. The position on confidentiality is as follows:

- By engaging with our services the service user is giving consent for Conwy Mind to access any relevant records that may be required for an accurate and ongoing assessment of need.
- Conwy Mind will share relevant information with other support providers and/or statutory services as required.

2. Procedure

The Director is the responsible authority for ensuring that Conwy Mind complies with matters of confidentiality.

It is the responsibility of Conwy Mind to familiarise all new employees and volunteers with this policy as part of their induction programme, and to ensure that they know what is required of them.

All employees and volunteers (including Trustees) are required to comply with this policy on confidentiality relating to third parties.

Conwy Mind will abide by the principles of data protection laid down in the DPA 1998. Written or computerised records will be stored securely in a locked cabinet or locked room, or under restricted or password protected access, so that only relevant staff can see them.

Examples of steps that could be taken to maintain confidentiality of service users and other members of staff are:

- Securing confidential information on computers with a password
- Turn the front pages of sensitive information/documents over on your desk when within the view of a third party.
- Maintaining a ”clear desk policy” at the end of business each day.

2.1 Service Users

All service users should be informed that information about them is being recorded, the subject of the records taken, why the information is being kept, who is going to use it and who has access to the information.

Information concerning service users should be kept to a minimum and must be factual, not speculative. If opinion is recorded, this should be noted as such.

Referral form will only request essential information in order to ensure that individuals' needs are met by the service.

Once a service user is no longer using a service for a period of two years, personal information other than that kept for monitoring purposes (sex, race, gender etc.), will be destroyed.

All service users may have access to their files / information recorded about them on request. If a user objects to information being kept on file, they should follow guidance in Conwy Mind complaints procedure.

Service users have the right to choose what to tell Conwy Mind. They should be made aware that if they disclose information to an individual that it might be necessary to share this information with other people within the charity. This is in order to provide the most appropriate help and support. Information about the identity and or/circumstances of people using our services will not be disclosed EXCEPT:

- If harm or threat of harm to anyone else is involved. Consultation within the organisation will occur if this happens and wherever possible the person giving the information will be told that it will be passed to other relevant agencies.
- When a person is referred to another agency with that person's consent.
- If it is necessary to discuss confidential information with staff if must be anonymous

2.2 Staff / Volunteers

The Director will ensure that all records are held securely. Access to these files will be confined to authorised staff on a need to know basis.

Each employee has the right to inspect the content of their own personal file and any data held on a computer. The request must be addressed in writing to the Director. When the request is granted, the information will be available to the employee within five working days and at an agreed time, in accordance with the Data Protection Policy.

Data Protection Act 2018

The Data Protection Act 2018 (DPA) gives the data subject the right to have access to their personal records held both manually and computerised. You can request to see what data Conwy Mind hold on your file, this should be done so in writing allowing thirty days for the process, should you require more than one copy of the data files there will be an administration fee of £25. It is the employees responsibility to notify Conwy Mind of any changes such as home address, name change etc, employees can do this by either notifying their Line Manager, the Administration and Finance Officer and/or the Director of Conwy Mind.

The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government.

The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
Everyone responsible for using personal data has to follow strict rules called 'data protection principles'. They must make sure the information is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Individual – Any confidential information shared by one person to a second remains confidential to that person.

Corporate – It is acknowledged that within normal working procedures of the organisation that certain information needs to be held collectively. Further it is considered good practise for anyone holding a position of trust regarding information about others, to be given support in terms of the work they undertake. Therefore, it is acceptable within these boundaries to share concerns/information. Provided it is done in suitable circumstances and is purposeful.

Within an organisation there may be exceptional circumstances under which it has been agreed that a confidence cannot be respected.

The general law does not give an absolute right to confidentiality except where there is a contractual provision to this effect. Legal and statutory requirements affecting Conwy Mind include, but are not limited to:

- Replying to certain specific enquiries from Government Departments e.g. Dept. of Employment or Dept. of Social Security, or the Inland Revenue.

- Passing on information on terrorist activities and information requested on road accidents involving personal injury, to the police.

- Reporting on trafficking in illegal substances that comes to the notice of staff or volunteers.

- Giving evidence in court, if a subpoena is issued.

- Where it is believed there is a risk to an individual's personal safety or a risk to a third party or third parties.

Giving information to the Police

Employees and volunteers have a duty in the public interest not to withhold information from the Police, such as the information described above.

Giving information concerning criminal activity of a serious nature should preferably be done with the knowledge of the person concerned and whenever possible with their cooperation but there may be circumstances where the risk to others is too great for this to be advisable or possible.

Duty of Care

Conwy Mind owes a "duty of care" to its service users. It may therefore be necessary to breach confidentiality where a service user is acting, or likely to act, in a way that could cause serious harm to him or herself or put other users at risk.

Conwy Mind also owes a more general duty of care towards members of the public. It may be necessary to pass on information to the police or statutory authorities where there is considered to be a serious risk to a particular person or persons, or to the public in general.

Where there is no legal obligation but there may be a "duty of care" to pass on information the decision will be of individual judgment. The following points of consideration should be used to help the decision made:

- Is the risk a real one?

- How great is the danger to self or to another person?

- Will the breach of confidentiality avoid the harm?

- Is there no other way of avoiding the harm?

The advice of the appropriate staff should be sought.

Where it is decided that information must be passed on this must be limited to those who need to know the information.

For Conwy Mind, such circumstances include, but not exclusively with reference to, information regarding child abuse or the abuse of vulnerable adults. Should such circumstances arise, it is important, if circumstances permit, to discuss this with the individual and to share the reason for its disclosure. If possible, it is desirable to encourage and support that individual in undertaking the act of disclosure themselves. Any such disclosure should only take place with reference to and the support of the line manager or Chairman.

Under the prevention of Terrorism Act 1984 there is a legal duty on all citizens to divulge to official bodies any information relating to acts of terrorism. The Criminal Law Act 1967 makes it clear that a criminal offence has not been committed, "if someone fails to pass on knowledge of a crime". It is a criminal offence to assist a criminal, or would be criminal, to share in the proceeds of a criminal act or to deliberately mislead the police.

Terrorism, child abuse and the abuse of vulnerable adults are just three examples of when such disclosure is necessary. There may be other examples found during working practice.

Any issues of a particularly sensitive and confidential nature which are discussed in meetings of the Executive Committee or sub-group will be recorded separate from the minutes as a confidential report and circulated only to the Executive Committee and those involved.

Everybody involved in the organisation should be aware of their right to refuse to receive inappropriate information of a confidential nature.

Appropriate steps must be taken by all involved in the organisation to ensure that paper documents are stored appropriately and securely.

All computer documents and files relating to confidential issues will be password protected. The requirements of the Data Protection Act will apply to all information on the computer.

The law requires that certain types of information must be made available to members, auditors, the Charity Commission, Companies House and the Public. The organisation may itself decide to be open about other types of information. Each employee and member of the Executive committee needs to be aware of which information the organisation is open about and which information must be kept confidential.

If in doubt, information should be kept confidential until the situation has been clarified with the Director.

Human Rights Act, article 8 "Private and family Life"

8.1 Everybody has the right to respect for his private and family life, his home and his correspondence.

8.2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The form included below is to be used on all occasions where information is shared about a service user without the service user's consent. A record of these forms will then be stored in the Confidentiality Form file in the locked filing cabinet in the office.

Document information

Policy author:	Jacky Baldini	Trustee
Version and status:	V1.0	
Date of Creation:	June 2019	
Date of Authorisation:	July 2019	
Review date:	July 2021	

Change Log

Version	Approved By	Changes

Information Shared Without Consent

The following information was shared with (contact name) ----------

Of (name of organisation) ----------

The information shared was:

The information was shared, without consent, for the following reason:

Name of worker: ----------

Signature: ----------