Confidentiality Policy & Procedure

1.Background

During the course of everyday working, CW Mind staff and volunteers handle a great deal of information, in both paper and electronic formats. Some of this is the personal data of service users, staff, volunteers, supporters, donors and trustees and is covered by our Data Protection Policy (POL14).

Information about CW Mind and its work is also sensitive and confidential and could, if disclosed, have adverse implications for the organisation.

CW Mind aims to strike a balance between encouraging openness, avoiding unnecessary secrecy and bureaucracy, and ensuring individual privacy is respected. The confidentiality policy and associated procedures set the framework within which personal and any other potentially sensitive information is to be collected, stored, handled and disclosed.

Most breaches of confidentiality happen through lack of thought or consideration of the possible consequences, or a lack of private or secure facilities. The best protection against breaches of confidentiality is to keep to a minimum the number of people who have access to sensitive information. Anyone worried or distressed by something they hear or read should seek guidance and support from their manager.

2.Scope

The policy, and procedures in this policy, are applicable to all staff, volunteers,

trustees and any contracted third parties. If you are in any doubt about the application of this policy, please seek guidance from your line manager or head office.

This policy is designed to work with and support various codes of professional conduct that are applicable to the type of the work undertaken by CW Mind as well as to support guidance used by CW Mind on safeguarding children and vulnerable adults, data protection and use of information technology. It should be read in conjunction with CW Mind's Data Protection Policy (POL 14).

If a situation arises where there is a potential conflict between the code of practice and this policy, please seek guidance from your line manager or the organisation's Caldicott Guardian.

3.Policy Statement

The overriding aim of this policy is to protect and promote the best interests of individuals and CW Mind, and any question concerning confidentiality should be answered by reference to this principle.

When working with CW Mind, you must:

- Treat all personal data and sensitive organisational information as confidential to CW Mind.
- Comply with the law regarding the protection and disclosure of information (including Data Protection Legislation, e.g. GDPR) and our policies, including our Data Protection Policy.

Any breach of this policy could have very serious consequences for an individual or for CW Mind and will be treated as a serious disciplinary matter.

4.Information to be kept confidential

All personal data and confidential information about CW Mind, our partners and other third-party organisations must be kept and handled confidentially, whether the information has been received formally, informally or discovered by accident – anything seen or overheard accidentally is still personal data.

Broadly, this includes:

- Any information which relates to or is about an identified or identifiable individual, i.e. their name linked with any other information about them (address, telephone number, etc).
- Anything else provided to us in confidence by third parties and that is not a matter of public record.

- Sensitive organisational information that could be used to damage CW Mind.

5.Handling Confidential Information

All personal data should be treated in the strictest confidence and in accordance also with CW Mind's Data Protection Policy (POL14).

Your work is likely to bring you into contact with information that is personal to someone or organisational information that is not yet ready for distribution. Anyone worried or distressed by something they hear or read should seek guidance and support from their line manager.

When handling personal data and other confidential information of CW Mind, its partners and other third-party organisations, always follow a few simple rules:

- Even in the most innocent of conversations, do not discuss any part of your work that could cause either an individual or CW Mind embarrassment or harm.
- Be aware of who else might be listening, particularly in areas open to the public.
- Get into the habit of checking and clearing your work area and locking your desk and filing cabinets before leaving at the end of each day. It is acceptable to leave some work out but lock away anything confidential or even for limited circulation.
- Always lock your computer screen if you leave your desk during the unattended and log out completely when you have finished for the day.
- Never leave confidential information unattended; either put it in an envelope marked confidential or lock it away. If someone comes near you while you are working, discreetly cover the material or ask the person to leave.
- If you need to take sensitive documents away from the office, seek permission first.
- Do not read or process confidential documents on public transport.
- Do not leave confidential documents unattended in car parks or public places.
- Store documents securely at home and do not show them to other household members.
- Remember that information in the wrong hands can cause a lot of damage and unnecessary stress.

In discussions or meetings:

- Only disclose information that is relevant.
- Do not discuss personal information about another person – refer to service users by initials wherever practical.
- Do not disclose the name of a person making an allegation about someone

else without the complainant's consent.

When entering into correspondence with an individual that will contain personal data (including, for example, sensitive information such as health data), you should:

- Check with the person concerned that they can be written to at their home address or make arrangements for letters to be collected or sent elsewhere.
- Check whether correspondence should be marked 'private and confidential'.

When collecting and/or recording information about a person:

- Offer a private interview wherever possible but in instances where, at the request of the service user, the meeting is held in a more public space, every care should be taken to ensure that the conversation is not overheard.
- If the conversation is over the telephone and someone else might hear, do not repeat aloud any personal information. If necessary, ask the person to say it again.
- Explain first why the information is needed and how it will be used and obtain their consent if this is required. If CW Mind needs to collect it for legal or other purposes, the individual must be informed.
- Staff/volunteers should ensure that service users have a copy of the relevant privacy notice or refer them to the privacy statement on CW Mind's website for more information.

When collecting sensitive personal data (for example, health information), in some cases we will need to have explicit consent – this can be oral or written statement. Staff/volunteers should also explain:

- Who will have access to it?
- The implications of not giving the information.
- Any special procedures for protecting particularly sensitive information.
- If the individual does not agree, do not record or pass on the information. Explain this and its implications to the person.
- Do not ask questions that are not relevant.

Ensure that any personal data you record is:

- Factual and relevant. Keep expressions of opinion to a minimum and make sure they are fully justifiable on the basis of the factual information.
- Accurate. Wherever possible, take notes during interviews and conversations and use the person's own words. Check the record with them if possible. Where appropriate, ask for and examine supporting documents and record this on the file.
- Comprehensive and clear. Another staff member might have to form a judgement from the information and the person concerned may wish to read it.

Handling incoming information

Any envelopes marked ‘confidential’, ‘personal’ or ‘private’ should be passed on to the addressee only unopened. Where this is addressed to a member of staff by name, the post will be opened by a senior member of staff/designated administrative personnel.

- If anything of a confidential nature is not in an envelope, put it in a sealed and appropriately marked envelope before passing it to the addressee.
- If confidential correspondence is opened by mistake, it should be resealed and clearly marked who opened it in error.
- Any confidential correspondence or messages should be placed in a sealed envelope marked confidential; this includes any rent statements or arrears statements.

Typing and administration

- The administration, typing, printing, photocopying, faxing and filing of confidential information must only be carried out by employees or volunteers who are familiar with CW Mind confidentiality procedures.
- The following precautions should always be taken:
    - Take care to securely destroy all unused rough work and any spare copies.
    - When photocopying, do not let anyone else read the documents, make only the required number of copies and check that nothing is left in the machine afterwards.
    - When faxing, ensure the first page clearly shows the contents are confidential, the fax is sent by a designated person, and alert the recipient in advance to collect it from the machine immediately. Place any incoming confidential faxes arriving, when the recipient is not present, in an envelope marked confidential before passing on the fax to the recipient.

Working with computers

- No disks, CDs, memory sticks or other portable storage media should be used to store personal data unless encrypted and unless authorised by a member of CW Mind’s senior management team.
- All/any personal data stored on laptops to undertake outreach or remote services should be encrypted and appropriate passwords should also be set on tablets and mobile phones.
- Computers should be locked, or users should log out to prevent access if computers are left unattended for any length of time.
- When using email addresses, external recipients should not be grouped unless permission has been obtained.
- The BCC facility on email should not be used as a mechanism for sharing or distributing personal data.

Keys

- All keys to CW Mind properties must be kept securely with spare keys kept in a key cabinet or drawer that is kept locked. Do not keep keys in unlocked drawers.
- Filing cabinets and desk drawers with confidential information should be kept locked and keys kept securely with spare keys kept in a locked key cabinet. Do not keep keys in unlocked drawers.

6.Access to sensitive information

Staff will generally have access to all information that they genuinely need to know to carry out their work and are under a duty to respect the confidentiality of all personal data held by CW Mind.
Staff should have explained or made privacy information available to the individual to explain the purpose of recording the personal data, how that information will be used and whether it will be shared with any third parties when they collect the information. If this causes concern, special arrangements for recording and access will be made available where possible. If concerns cannot be allayed, it may be impossible for CW Mind to undertake a particular activity for a given individual.

7.Information obtained by service users

Service users involved in group work/peer support activities are likely to be aware of personal data about other service users and should be made aware of the need to respect their right to privacy.

Service users involved in group work/peer support activities will be asked to sign a confidentiality agreement to confirm their commitment to confidentiality prior to their involvement, outlining their responsibilities and disclosure risks from other members.

CW Mind will make service users aware of their responsibilities under these circumstances and that they are responsible for ensuring they comply.

8.Access to Confidential Information

All employed staff, sessional workers and volunteers must sign a confidentiality agreement before being given access to CW Mind information assets. CW Mind will make service users aware of their responsibilities.

9.Sharing with third parties

External agents and contractors who process personal data and other confidential

information on behalf of CW Mind must be made aware of CW Mind's information governance requirements; what they can and cannot do, and who they should contact if things go wrong.

All agents and contractors in receipt of CW Mind confidentiality information should complete and sign a Data Sharing Agreement at the outset of the contract being established. Where those third parties are specifically processing personal data (as a data processor) for CW Mind, the contract should also set out that CW Mind is the data controller and the third party is the data processor and the respective obligations of both parties under the Data Protection Legislation.

CW Mind managers responsible for contracting with their party organisations where access to CW Mind's information assets is required, should undertake a due diligence check and risk assessment to establish the adequacy of the third party's confidentiality, security and information governance assets.

10.Managing a breach of confidentiality

All staff should help to prevent accidental disclosures occurring by regularly pointing out that certain information is confidential and checking that people have understood. If accidental disclosure occurs, the responsible CW Mind manager should take swift action to minimise the damage. They should find out who knows about the incident, talk to them and remind them of their duty to maintain confidentiality.

Any breach must be reported immediately to the Senior Management Team.

11.Roles and responsibilities

The Chair is responsible for gaining assurance that confidentiality is managed appropriately within the organisation and that adequate resources are made available to implement this policy.

The Chief Executive Officer is responsible for ensuring that all confidential information processed by CW Mind is handled in line with this policy and associated procedures and for providing assurance of such to the trustees.

The Quality & Information Governance Lead is responsible for providing advice in relation to this policy as should be the first point of contact for any data protection queries, subject access requests or the reporting of data protection breaches

within the organisation. See also POL 14 – Data Protection Policy.

The Caldicott Guardian is a senior person who is responsible for ensuring that the personal information about those who use its services is used legally, ethically and appropriately, and that confidentiality is maintained.

Line managers will be responsible for ensuring that all CW Mind staff working in a service delivery role have read this policy and are working to the required standard. They will ensure that a high standard of record keeping is maintained by conducting regular audits and will provide training for staff alongside the organisational training in this area.

All CW Mind staff or volunteers with access to confidential information have responsibilities to ensure that they comply with this policy and with any guidance subsequently produced.