



CONFIDENTIALITY POLICY

1. Introduction

A Confidentiality Policy is necessary for the following reasons:

- 1.1 To protect clients, employees and volunteers from the possibility of information about them being passed on to individuals or organisations who have no right to that information.
- 1.2 To reassure clients, employees and volunteers that good care will be taken with information which they give to Mind and to be clear as to the circumstances when information can be shared with others.
- 1.3 To 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.
- 1.4 To assist Mind employees and volunteers to comply with legal and statutory requirements for the disclosure of information.
- 1.5 To reassure clients wishing to make a complaint to or about 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.
- 1.6 To comply with relevant legislation and standards required by accreditation to certain quality marks and codes of practice.
- 1.7 This policy should be read in conjunction with Mind in Croydon's Information Governance Policy and Privacy Policy (UK GDPR policy).

2. General confidentiality statement

- 2.1 All Mind employees and volunteers are required to respect the right of clients and of other employees and volunteers to privacy and confidentiality as far as possible within the constraints of legal requirements and the safety of other people.
- 2.2 Absolute confidentiality cannot be guaranteed and this will be made clear to clients at the earliest possible opportunity.
- 2.3 Where it is thought necessary to pass on information to another individual or organisation this will be assessed on the basis of their application and full consideration of whether there is a legal duty to disclose information. The client will be advised that information has been requested, and by whom. Where possible, the consent of the person about whom the request has been made will be sought, if at all possible. The client will be advised that they should seek legal advice if they strongly object to information being passed to a third party.
- 2.4 This policy covers not only information given deliberately by the person concerned or by other people about the person, but also information acquired accidentally or through observation.

3. Circumstances in which confidentiality may be breached

3.1 Legal and Statutory Requirements

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 Mind include, but are not limited to:

- Reporting notifiable diseases to the Director of Public Health where appropriate.

- Reporting accidents at work, in certain circumstances, to the Health and Safety Executive.
- Replying to certain specific enquiries from Government Departments e.g., Department of Work and Pensions, or HMRC. Not all such enquiries are covered by statutory requirements so a check on the legal status of the request should be made before supplying information.
- Passing on information on terrorist activities and information requested on road accidents involving personal injury, to the police.
- Giving evidence in court if a subpoena is issued.

3.2 Duty of Care

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

Mind in Croydon 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.

Mind in Croydon employees and volunteers share with all citizens a duty of care towards children and vulnerable adults.

If Mind in Croydon workers know or suspect that a child is at risk they should contact Croydon Council's Single Point of Contact (SPOC) Team. If Mind workers know or suspect that a vulnerable adult has been abused Social Services Care Management must be informed in accordance with Croydon's Safeguarding procedures. (Please see Mind in Croydon's Safeguarding Policies).

3.3 Giving Information to the Police

There is no absolute duty to provide the Police with information except in the case of suspected or actual terrorism. However, Mind in Croydon's policy is that its employees and volunteers have a duty in the public interest not to withhold from the police any information concerning criminal activity of a serious nature. This 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.

4. PASSING ON INFORMATION TO OTHERS

4.1 Where there is a legal duty to pass information to others, such information will only be passed after discussion and approval by the Chief Executive. Junior staff are not permitted to pass on such information. Where there is no legal obligation but there may be a duty of care to pass on information the decision whether or not to do so will in the end remain one **of individual judgement**. Points for consideration are:

- 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 line manager or project leader should be sought and, except where there is a legal requirement to breach confidentiality, a

senior staff member (Chief Executive and Director of Services) must be informed and they will inform the Chair.

4.2 Where it is decided that information must be passed on to another individual or organisation the basis on which disclosure is to be made must be clear and unambiguous. Those disclosing the information must first have an understanding as to the intended use of the information requested and by whom.

4.3 Requests from statutory bodies must be submitted in writing, even when there is a legal obligation on Mind to comply with the request.

5. CARE OF INFORMATION

Mind volunteers and employees will take care:

5.1 Not to be overheard when discussing confidential information on the phone, or with the client or appropriate staff.

5.2 Not to leave information lying around and to keep confidential information in locked filing cabinets when not in use.

5.3 To keep records which include no more than the minimum information required.

5.4 To destroy information when it is no longer required.

6. Sharing with third parties

6.1 External agents and contractors who process personal data and other confidential information on behalf of Mind in Croydon must be made aware of Mind in Croydon's information governance requirements and who they should contact if things go wrong.

6.2 All agents and contractors in receipt of Mind in Croydon's confidential 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 Mind in Croydon, the contract should also set out that Mind in Croydon is the data controller and the third party is the data processor and the respective obligations of both parties under the Data Protection Legislation.

7. COMPLAINTS

People who wish to make a complaint either to Mind in Croydon about another agency or individual or about an aspect of Mind in Croydon services or Mind in Croydon' employee or volunteer may be concerned about the confidentiality of information they are giving. The preservation of confidentiality will be given high priority, subject to the exceptions listed above in section 3 and/or if it is necessary to breach confidentiality in order to properly investigate the complaint. The permission of the complainant will always be sought for this but in cases where the welfare of the complainant or other people is seriously at risk it may be necessary to breach confidentiality even if that permission is withheld

8. ACCESS TO INFORMATION

8.1 Clients have a right to see their personal files. Our Privacy Policy (UK GDPR) gives further details about how to deal with data requests etc.

9. OTHER MIND POLICIES

This policy should be read in conjunction with other relevant Mind policies e.g. Complaints Procedure, Safeguarding, Information Governance and Privacy (UK GDPR) policy.

10. REVIEW

This policy will be reviewed annually

Reviewed and Updated by the Board of Mind in Croydon – Sep 2023

APPENDIX A Caldicott Principles

The Caldicott Principles revised 2013 are:

Principle 1: Justify the purpose(s) for using confidential information

Every proposed use or transfer of confidential information should be clearly defined, scrutinised and documented, with continuing uses regularly reviewed by an appropriate guardian.

Principle 2: Use confidential information only when it is necessary

Confidential information should not be included unless it is necessary for the specified purpose(s) for which the information is used or accessed. The need to identify individuals should be considered at each stage of satisfying the purpose(s) and alternatives used where possible.

Principle 3: Use the minimum necessary confidential information

Where use of confidential information is considered to be necessary, each item of information must be justified so that only the minimum amount of confidential information is included as necessary for a given function.

Principle 4: Access to confidential information should be on a strict need-to-know basis

Only those who need access to confidential information should have access to it, and then only to the items that they need to see. This may mean introducing access controls or splitting information flows where one flow is used for several purposes.

Principle 5: Everyone with access to confidential information should be aware of their responsibilities

Action should be taken to ensure that all those handling confidential information understand their responsibilities and obligations to respect the confidentiality of patient and service users.

Principle 6: Comply with the law

Every use of confidential information must be lawful. All those handling confidential information are responsible for ensuring that their use of and access to that information complies with legal requirements set out in statute and under the common law.

Principle 7: The duty to share information for individual care is as important as the duty to protect patient confidentiality

Health and social care professionals should have the confidence to share confidential information in the best interests of patients and service users within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Principle 8: Inform patients and service users about how their confidential information is used

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant and appropriate information - in some cases, greater engagement will be required.

<https://www.gov.uk/government/publications/the-caldicott-principles>