Mind in Haringey

Confidentiality Policy

Date: September 2014

Mind in Haringey
Confidentiality Policy – Table of Contents

Confidentiality Policy

It is necessary to collect and keep a certain amount of information about our service users. Our confidentiality policy aims to safeguard privacy and ensure appropriate access to information. We therefore respect their rights to confidentiality and do not, except in specific circumstances set out in guidelines below, disclose information given to us to third parties. In order to maintain confidentiality the following principles apply.

- We collect information on a "need to know" basis. This means we only collect and keep information which is necessary. For example information which assists decision making, effective management and service provision and planning.
- Access to information held on a service user is restricted to Mind in Haringey staff and the service user. Within the organisation only the member/s of staff dealing with the service user should see their information. Information is not made available to third parties without the informed consent of the service user. Limited details may be given in some circumstances and these are detailed below.
- When collecting information from a service user we should always inform them why information is required and the use to which it will be put.

All staff are expected to act in accordance with this policy which applies to service users accessing services or information. Contractors working for the Mind in Haringey are also required to comply with our confidentiality policy.
The processing of information is governed by the Data Protection Act 1998 and the Human Rights Act 1998. The confidentiality policy is compatible with the legislation but staff members should ensure they are familiar with both Acts. Summaries of the Acts are available on the intranet.

Storing Information

The only staff who should access the information held on a service user are the service user and the staff dealing with them. Others may accidentally see written information, e.g. receptionists opening mail, or overhear phone conversations etc. In these cases it is equally important to respect confidentiality. Follow these guidelines to ensure confidentiality is respected:

Written Information

Ensure notes of interviews/meetings with service users are factual, observable and objective. Do not record unsubstantiated opinions, derogatory remarks. All written information must be accurate and justifiable. With very few exceptions, the service user has a right to see all information held about them.

Record the source of all information provided from an external agency or individual. We should, wherever possible, be able to identify the source of all written information about a service user. Again the service user has the right to be informed of the source of information held about them.

No confidential information should be accessible to any stakeholder.
If confidential information is sent in the internal mail, seal the envelope and mark it private and confidential.
Take care when throwing information away - if necessary consider shredding paper.

Take care when providing paper to be used for scrap - check it does not contain confidential information.

Discussions and meetings
When discussing a service user's personal information in a meeting only disclose information relevant to the case.
Be aware when discussing cases in the office that others with no involvement in the case may be able to overhear e.g. at reception, in an open plan office or corridors. Make sure discussions happen in an appropriate place.

Outside Work
Remember to respect confidentiality outside work as well as in work. This applies to information acquired out of work and at work.

Inside Work
Limited information about service user and staff details are acceptable to share internally if other staff are expected to assist or deal with situations involving service users and or visiting employees. E.g. service users or providers visiting the building in connection with services provided by Mind in Haringey. e.g. Name address and contact details for cancellations and confirmation of appointments, and those posing a risk to staff.

Reports
Committee reports concerning individual service users must not name the service user, but retain anonymity. In the few cases where this is not possible e.g. appeals to complaints, information is given in strict confidence. Confidential reports included as part of a wider non confidential agenda will be marked confidential and photocopied on coloured paper.

Sensitive Information
Take particular care in relation to sensitive information such as medical information. For example disclosure of someone's HIV status would never be acceptable.

Advocacy advisors and counsellors, as well as activity leaders and project workers, may have access to more detailed and private information on service users e.g. application forms, medical and health details, benefits and income information. Particular care must be taken in keeping the minimum amount of information necessary and respecting the service user's right to confidentiality.
Do not disclose the name of a service user making an allegation about a neighbour dispute or harassment without the complainants consent.

Putting Staff at Risk
On some occasions staff are aware that particular service users may present a risk to staff. For example where there has been threatening or violent behaviour in the past. Information about potential risks should be passed on to contractors if they are visiting the service users concerned. Details of the procedure for service users posing a risk can be found in the Risk Assessment Policy.

Requests for information – by the service user
Service users have a right to inspect information kept about them. If a service user asks do to so, you must ask them to send a letter of request and return it to you. The letter must be forwarded to the team that the service users query relates to. If the query is not specific (for example the service user may request to see the whole of their file) then this is dealt with by the manager of that service.

The identity of the service user must be proved, so the staff member dealing with the query must ensure that the form is signed, and verify their signature against the records that we hold. If there is doubt about their identity, or there is no signature record available, then further proof must be sought.

Examples of satisfactory proof:

- Driving Licence
- Passport
- Medical Card
- Pension Book
- Cheque or Credit Card
- Formal Identity Card (not bus pass or similar)

The necessary arrangements must then be made. The relevant sections of the file can either be copied for the service user or inspected during a home visit. The information must be provided to the service user within 40 days of the form being received and proof of identity determined.

When a request for information has been responded to the staff member should send a copy of the letter to the Director along with a memo summarising the action taken.

Third Party references

Where the requested information includes personal information on another individual this is classed as a third party reference. You need to consider whether to release that information to the service user as you may owe the third party a duty of confidence. For example there may be a letter on file about the service user by someone complaining that they have been harassing them. In this case the person making the complaint has the right not to have their name revealed to the alleged harasser, and you would have to remove the letter.

Other information held on file which identifies a **third party should be edited** so as not to reveal the third parties identity or you can obtain the third parties consent to the disclosure. In all cases go through the file before the service user inspects it and review any third party references.

Notes that are written by a member of staff reporting on information given by another party are also classed as third party information. Again, this information may be shown to the service user, but it should not reveal the third party (unless their consent has been obtained).
You must be able to justify any information that you have removed or edited from a file before passing it to a service user. If you are unsure then advice should be sought from your line manager.

Right to correct information

Service users have the right to comment on the information held on file. If there is a disagreement, note this on the file. If the information is incorrect it can be altered on the service user's written request. The staff member dealing with such a request should ensure that the details to be corrected or deleted are those which can be changed. Examples are dates of birth, spelling of names, members of household etc. Requests cannot be made to change information such as a nomination agency, date Notice of Seeking Possession served etc, unless there has actually been an error on the Group member's part.

Service users also have a right to ask for incorrect data held on computer to be corrected or amended.

Requests for information – by external organisations
It is not uncommon to receive requests for information on our service users from other organisations. Many requests will simply be to confirm a service users name and address. In general we do not give out information about a service user to third parties. There will however be some circumstances when we will give out this information, which is outlined in the guidance below. Always find out why information is required.

If an organisation or individual requests a former service user's new address do not disclose the address. If we have the address forward any requests. Enclose a covering note explaining that neither their address nor other information has been given out.
If an organisation or individual requests information on the phone, unless you are sure of their identity, ask for their name and number and phone back.
If an official caller to the office requests information on a service user first ask for ID.
Do not provide information to individuals making requests in a personal capacity.
It is impossible to cover every type of request from every possible organisation but the following acts as a guideline. If you are in doubt, refer to your team leader or manager for advice. There is no legal obligation to disclose information to statutory authorities except in the cases outlined below.

Police
If the request is to confirm whether a certain person lives at a certain address, provide the information. If there is no court order no other information has to be provided. Find out why the information is needed and refer the request to the Team Manager who will exercise discretion in deciding whether to provide further information.
If there is a court order insist on seeing it. You are obstructing the course of justice if a court order for information is ignored.

- In some boroughs an Information Sharing Protocol has been set up between the Trust and the police. This is a formal agreement allowing information to be disclosed by either party on request. For example, the police may contact us to ask if there have been complaints of drug-dealing at a particular property, or the Trust may wish to obtain details of drug raids for the purposes of possession action.

Solicitors and other legal advisors
If a solicitor or other legal advisor requires information which is necessary for legal proceedings or the provision of legal advice they are entitled to this information under section 35 of the Data Protection Act 1998. Staff members should ensure that only information necessary for these purposes is revealed. For example, a service user needing advice on possession proceedings for rent arrears would not need to see documents relating to harassment. Solicitors requesting information that will not be used for the purposes of legal proceedings or the provision of legal advice will need to provide the service user's written authorisation.
.
Social Services & MHT Professionals
A service user's name and address can be provided. In cases of suspected abuse or neglect we may decide it is necessary to disclose information. Consult with Team Managers in deciding whether to pass information onto social services. Information

should only be given in the best interests of the parties involved. However, we will inform social services if we believe that a child or vulnerable person may be at risk.

Press

Refer all requests from any media to **your Director or Chair.**

MPs or other advocates contacting the Group on behalf of a resident

Information cannot be provided to MPs or other advocates contacting the Group on behalf of residents without the written authorisation of the service user. Refer all requests to **your Director or Chair.**

Breaches of Confidentiality

Breaches often occur as a result of thoughtlessness and lack of awareness of the potential consequences of inappropriate disclosure. However, to the service user concerned the effect is the same whether the breach is intentional or accidental. All breaches will be taken seriously and are potentially a disciplinary issue.

Further Guidance

The Management Team are available for guidance on processing data that relates to service users. Staff members should email their manager providing full details of the case. The Manager can then contact our employment advisors for advice if necessary. Written information on the Human Rights Act and the Data Protection Act are available on the internet.