

Leeds Mind Policy



For better
mental health

Data Protection Policy

Why do we need this policy?

The keeping of personal records and personal data is covered by the 1998 Data Protection Act which replaced the Data Protection Act of 1984 and came into effect in March 2000. This means we must follow certain principles in relation to the data we hold.

Who does it apply to?

This policy applies to all staff, students, volunteers and Executive Committee members of Leeds Mind.

Introduction

All organisations need to keep certain records, some because the law requires them, and some for internal purposes. Personnel records are necessary for the formulation and implementation of employment policies and procedures for recruitment, training, promotion, dismissal etc. Organisation planning depends on information, and personnel planning equally depends on effective, accurate record keeping to recruit, train and develop staff to their full potential, and be as effective as possible within the organisation, thereby making a strategic contribution to its goals.

Policy

Leeds Mind is committed to fulfilling its obligations under the Act in respect of all personal data (information about identifiable, living individuals) held in manual records, on computer systems and any other format.

Definitions:

Personal data is: *“Information about identifiable (named), living individuals recorded with the intention that it be processed automatically by equipment, or recorded as part of a relevant filing system.”*

“Sensitive” personnel data

Certain data is classed as “sensitive”, including data around racial or ethnic origin, religious or political beliefs, Trade Union membership, health, sexual life and criminal record.

Before holding or using “sensitive” data you need the Data subject’s “explicit” consent – such as a signature on a statement which sets out the data to be held, the purpose for which it is held, anyone it may be disclosed to and other relevant information. Sensitive personal data

should be kept separately from “personal data” and only collected and processed for specified purposes e.g. ethnic monitoring

The following principles laid down in the Data Protection Act will apply when we handle personal information and apply whether the records are paper or electronic.

Overall principles:-

1. Personal data is only processed with an individual’s knowledge
2. Information will only be seen by those who need to, to enable them to do their jobs
3. Only information we actually need is collected and processed and held only for specified and lawful purposes.
4. Data actually held must be adequate, relevant and not excessive in relation to the purpose(s) for which it is held.
5. The information kept will be accurate and up to date and will be reviewed regularly to ensure its accuracy
6. The information will not be kept longer than is necessary for the purpose it is collected (see Appendix 1. Record Retention)
7. Personal data on an individual shall be disclosed and/or produced to him/her within 28 days. An administration cost of up to £10 may be charged. The data must be corrected or erased if inaccurate.
8. The information is protected against unauthorised and/or accidental disclosure, access, alteration or destruction
9. Information will not be transferred to countries without adequate protection.

Individuals also have the right to access data that is held on them and rights to claim for damages if various offences occur.

Purpose for holding data

1. Staff Administration

- Information for the purposes of appointments or removals, pay, discipline, Superannuation, work management or other personnel matters relating to staff.
- Personal data necessary for staff administration – statutory employment records and/or information required for operational management and administration.
- Information from disclosures (other than with the consent of the data subject) is restricted to those third parties which are necessary for staff administration.
- Data retention – only for as long as it is necessary for staff administration.
- Records held in any project e.g. supervision notes/appraisals.
- Other records - “one off” records for a particular purpose e.g. Disciplinary or Grievance where it is not reasonably practicable to keep the whole record in one file.
- Recruitment paperwork where a separate file may be created for the purposes of that process.

2. Membership Administration

3. Fundraising

4. Service user records- Information such as care plans and referral information

5. **References-** Confidential references given **by** an employer are excluded from disclosure (but not references given **to** the employer)
6. **Mailing lists** - to provide information e.g. IMH

Registering

Leeds Mind will register as a “data user” with the Data Protection Registrar. This registration is renewed annually and allows us to process certain personal information following strict guidelines.

Ownership and Accountability

The ownership of personnel employment records rest with Leeds Mind. In order to ensure clear accountability for the proper conduct of such records it is important to identify who may establish and maintain them and to this end personal employment records (personnel files and payroll information) may only be established and maintained by:-

- The Senior Management Team
- Project Managers
- HR Director and Personnel Officer

Service user records can only be established and maintained by the Project Managers and identified workers.

Information that cannot be included

Information, data or other material that cannot legitimately be shown to be related, directly or indirectly to the employment of the employee e.g. marital status and religious beliefs.

Format, location and security of Records

1. Records must be kept in a form that is (by and large) chronological, easily readable and auditable.
2. Records must be kept in a secure location with controlled access for only those who are authorised to have access. It is the responsibility of the persons named (see ownership and accountability) to ensure that all data is kept securely and that there is no unauthorised or unlawful processing of personal data. There must also be sufficient security to guard against accidental loss
3. Security measures to be taken for ensuring data security:-
 - Locking doors where computer equipment is held
 - Locking cabinets
 - Set screen savers on all PC's to ensure that 3rd parties do not have access when the designated user is away from their desk
 - Ensuring information is not left lying around
 - Restricting physical access
 - Authorised and identified users
 - Software controls (passwords) – which may include monitoring and logging access to assist detecting and investigating breaches
 - Having a back up plan in case of personal data being lost through fire, flood, accident or other reason

Consent

For prospective and new employees/workers consent will be obtained by a specific signed declaration in the Employment Application form and the Contract of Employment issued on appointment

Access to data

1. Staff and Service users have the right to access data held on them (including data in manual files from 24 Oct 2001) subject to certain procedural conditions.
2. They have the right to be informed of and have access to any records kept within 40 days of giving **written** notice.
3. The manager will then respond giving written confirmation of the date, time and place at which access will be provided.
4. A fee of £10 will be charged for each access request payable in advance.
5. For viewing/access the information will be at its kept location, in the presence of a person nominated by a member of the Senior Management team.
6. HR will be informed of any request to access personal data
7. Anyone may, within reason, request one copy of any or all the contents of the records. A record will be made of any copies requested and where possible, provided, including the date, time and place together with the name of the person providing them.

Right to challenge

1. Staff and service users may challenge the accuracy of an entry in their record, and if found to be inaccurate shall be entitled to have that entry removed or corrected.
2. They may challenge the legitimacy of making or keeping particular data or other information in the record.
3. If an employee/service users believes that the data held on them is inaccurate they should approach their Line Manager – for service users this will be the Project Manager, who will investigate the claim in consultation with the appropriate Director and HR. The employee/service user will receive a written response within 21 working days stating what action has been taken or will be taken or stating the reasons for regarding the concerns as unjustified. If the employee/service user is still not satisfied they have the option of making an official complaint via the Leeds Mind Complaint's procedure.

References

1. All references, oral or written, given in respect of a member of staff of Leeds Mind should only contain information that is factual or is an honest opinion or judgement that is capable of being demonstrated as being reasonable by references to actions, events or circumstances - must be "*true accurate and fair*".
2. References given formally on behalf of Leeds Mind should be given on headed paper and signed by the author. Where a proforma is completed this must be authenticated by the official company stamp and/or the signature of the author.
3. A copy of (including proformas) references must be taken and kept in the staff member's personnel file.
4. Staff will be entitled to have access to references received, on request **if** the provider of the reference has consented and there is no other substantial reason from Leeds Mind to do otherwise.

5. References already received at the implementation of the date of this policy and understood at the time of writing to be “confidential” shall remain so.
6. Confidential references given are exempt from subject access under the Data protection Act. Nevertheless they should be written in the knowledge that the receiver may seek consent to disclose the reference to the prospective staff member before/after they are engaged. Leeds Mind may or may not agree to such a disclosure.
7. All references should contain the statement:
“This reference is given in confidence and good faith and without any legal liability placed on this organisation or any of its employees”

Compensation

The data subject who suffers damage as a result of the failure of a data controller to comply with the Act may be awarded compensation

Retention of data

Records/data covered by this policy shall be retained for the relevant statutory period or as stated in the Leeds Mind policy on Document retention

Non Compliance with this policy

Non compliance with this policy will be treated as misconduct and will render the person liable to disciplinary action. All breaches will be fully investigated.

This policy will be reviewed every 2 years and in line with any legislative requirements

Other Leeds Mind policies that this policy dovetails with

Document Retention/Record Keeping
CRB policy/procedure
Employment of Ex Offenders

Further Information

ACAS – Personnel data and Record Keeping
The Information Commissioner's www.informationcommissioner.gov.uk)

Accessibility

If you would like a copy of this policy in a larger print, get in touch with us at Leeds Mind Central Admin by phone (0113 230 7608) or email (leeds.mind@leedsmind.org.uk) and we'll be happy to send you one.

**Date formally approved by
Leeds Mind Executive Committee: July 2006**

Date to be reviewed: July 2008