

Data Protection Policy

Document: <i>Data Protection Policy</i>	Page 1 of 7
Responsibility: <i>Lewisham LINK Executive Committee</i>	Version: <i>1.0</i>
Date of Issue: <i>23.02.10</i>	

Document Owner

Executive Committee

Lewisham Local Involvement Network

Document Status

Version	Comments/Reason for change	Date	By
1.0	Approved/Issued	23.02.10	Executive Committee

Contents

	PAGE
1 Introduction	4
2 General principles	4
3 Why information is held	5
4 Access to information	5
5 Storing information	5
6 Duty to disclose information	6
7 Disclosures	6
8 Data Protection Act	6
9 Breach of confidentiality	6

Document: <i>Data Protection Policy</i>	Page 3 of 7
Responsibility: <i>Lewisham LINK Executive Committee</i>	Version: <i>1.0</i>
Date of Issue: <i>23.02.10</i>	

1. Introduction

The Lewisham LINK's data protection policy is in accordance of the Data Protection Act 1998 which governs the use of personal information through the eight data protection principles. These principles require that personal information is:

- processed fairly and lawfully
- processed for one or more specified and lawful purposes, and not further processed in any way that is incompatible with the original purpose
- adequate, relevant and not excessive
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary for the purpose for which it is being used
- processed in line with the rights of individuals
- kept secure with appropriate technical and organisational measures taken to protect the information
- not transferred outside the European Economic Area (the European Union member states plus Norway, Iceland and Liechtenstein) unless there is adequate protection for the personal information being transferred

2. General principles

- 2.1 Lewisham LINK recognises that LINK colleagues gain information about individuals and organisations during the course of their work or activities. In most cases such information will not be stated as confidential and colleagues may have to exercise common sense and discretion in identifying whether information is expected to be confidential. This policy aims to give guidance but if in doubt, seek advice from the LINK Development Manager.
- 2.2 Colleagues are able to share information with the Development Manager in order to discuss issues and seek advice.
- 2.3 Colleagues should avoid exchanging personal information or comments (gossip) about individuals with whom they have a professional relationship.
- 2.4 It is not appropriate to discuss a person's sexuality (i.e. 'outing' a gay person) without their prior consent.
- 2.5 Colleagues should avoid talking about organisations or individuals in social settings.
- 2.6 Colleagues will not disclose to anyone, other than LINK Development Manager, any information considered sensitive, personal, financial or private without the knowledge or consent of the individual, or an officer, in the case of an organisation.
- 2.7 There may be circumstance where colleagues would want to discuss difficult situations with each other to gain a wider perspective on how to approach a problem. The organisation's consent must be sought before discussing the situation, unless the colleague is convinced beyond doubt that the organisation would not object to this. Alternatively, a discussion may take place with names or identifying information remaining confidential.

Document: <i>Data Protection Policy</i>	Page 4 of 7
Responsibility: <i>Lewisham LINK Executive Committee</i>	Version: <i>1.0</i>
Date of Issue: <i>23.02.10</i>	

- 2.8 Where there is a legal duty on Lewisham LINK to disclose information, the person to whom the confidentiality is owed will be informed that disclosure has or will be made.

3. Why information is held

- 3.1 Most information held by Lewisham LINK relates to voluntary and community organisations, self-help groups, volunteers, students, employees, executive body members or services which support or fund them.
- 3.2 Information is kept to enable Lewisham LINK colleagues to understand the history and activities of organisations in order to deliver the most appropriate services.
- 3.3 Information about ethnicity and disability of users is kept for the purposes of monitoring our equal opportunities policy and also for reporting back to funders.

4. Access to information

- 4.1 Although certain information is confidential, in certain circumstances, it may be passed to colleagues, line managers or the executive committee to ensure the best quality service for LINK participant and service users of health and social care services.
- 4.2 Where information is sensitive, i.e. it involves disputes or legal issues; it will be confidential to the LINK Development Manager and Chair. Such information should be clearly labelled 'Confidential' and should state the names of the colleagues entitled to access the information and the name of the individual or group who may request access to the information.
- 4.3 Colleagues will not withhold information from the LINK Development Manager unless it is purely personal.
- 4.4 Members have a right to see Lewisham LINK records held in their name or that of their organisation. The request must be in writing to the LINK Development Manager giving 14 days' notice and be signed by the individual, or in the case of an organisation's records, by the Chair or Executive Officer. Sensitive information as outlined in para 4.2 will only be made available to the person or organisation named on the file.
- 4.5 Employees and volunteers may have sight of their personnel records by giving 14 days' notice in writing to the LINK Development Manager.
- 4.6 When photocopying or working on confidential documents, colleagues must ensure they are not seen by people in passing. This also applies to information on computer screens.

5. Storing information

- 5.1 General non-confidential information about organisations is kept in unlocked filing cabinets with open access to all Lewisham LINK colleagues.
- 5.2 Information about volunteers, members and other individuals will be kept in filing cabinets by the Lewisham LINK staff team.

Document: <i>Data Protection Policy</i>	Page 5 of 7
Responsibility: <i>Lewisham LINK Executive Committee</i>	Version: <i>1.0</i>
Date of Issue: <i>23.02.10</i>	

- 5.3 Employees' personnel information will be kept in lockable filing cabinets by line managers and will be accessible to the LINK Development Manager.
- 5.4 Files or filing cabinet drawers bearing confidential information should be labelled 'confidential'.
- 5.5 In an emergency situation, the LINK Development Manager may authorise access to files by other people.

6. Duty to disclose information

- 6.1 There is a legal duty to disclose some information including:
 - 6.2 Child abuse will be reported to the Social Services Department
 - 6.3 Drug trafficking, money laundering, acts of terrorism or treason will be disclosed to the police.
 - 6.4 In addition colleagues believing an illegal act has taken place, or that a user is at risk of harming themselves or others, must report this to the LINK Development Manager who will report it to the appropriate authorities.
 - 6.5 Members should be informed of this disclosure.

7. Disclosures

- 7.1 Lewisham LINK complies fully with the CRB Code of practice (E File) regarding the correct handling, use, storage, retention and disposal of Disclosures and Disclosure information.
- 7.2 Disclosure information is always kept separately from an applicant's personnel file in secure storage with access limited to those who are entitled to see it as part of their duties. It is a **criminal offence** to pass this information to anyone who is not entitled to receive it.
- 7.3 Documents will be kept for a year and then destroyed by secure means. Photocopies will not be kept. However, Lewisham LINK may keep a record of the date of issue of a Disclosure, the name of the subject, the type of Disclosure requested, the position for which the Disclosure was requested, the unique reference number of the Disclosure and the details of the recruitment decision taken.

8. Data Protection Act

- 8.1 Information about individuals, whether on computer or on paper, falls within the scope of the Data Protection Act and must comply with the data protection principles as detailed at section 1 above.

9. Breach of confidentiality

- 9.1 Employees who are dissatisfied with the conduct or actions of other colleagues or Lewisham LINK should raise this with their LINK Development Manager using the

Document: <i>Data Protection Policy</i>	Page 6 of 7
Responsibility: <i>Lewisham LINK Executive Committee</i>	Version: <i>1.0</i>
Date of Issue: <i>23.02.10</i>	

grievance procedure, if necessary, and not discuss their dissatisfaction outside Lewisham LINK.

- 9.2. Colleagues accessing unauthorised files or breaching confidentiality may face disciplinary action. Ex-employees breaching confidentiality may face legal action.

Document: <i>Data Protection Policy</i>	Page 7 of 7
Responsibility: <i>Lewisham LINK Executive Committee</i>	Version: <i>1.0</i>
Date of Issue: <i>23.02.10</i>	