

BIRMINGHAM LINK

CONFIDENTIALITY AND INFORMATION SHARING

1. PURPOSE

This policy sets out to identify how Birmingham LINK performs its duties to keep Participant's and Elected Member's information safe and confidential, while, at the same time, not compromising its ability to share information where it is needed.

This Confidentiality Policy sets out the principles that must be observed, by all who have access to information.

2. POLICY STATEMENT

Birmingham LINK is committed to the privacy of all Participants and ELECTED MEMBERS. It expects all to handle all individuals' personal information in a sensitive and professional manner.

All Participants and ELECTED MEMBERS are under an obligation not to gain access or attempt to gain access to information which they are not authorised to have.

All Participants and ELECTED MEMBERS are expected to handle information in a way that also protects the security and reputation of the Birmingham LINK.

Most breaches of confidentiality happen through a lack of awareness of procedures, or insufficient attention to basic security, such as locking lockable cabinets, interview rooms or not-logging-off from computers.

Training in confidentiality will be made available to ELECTED MEMBERS, particularly Enter and View Managers.

The intentional or repeated accidental, unauthorised disclosure of any confidential information by Participant and ELECTED MEMBER will be subject to breaches of policy action. Any such action will take account of the confidential and possible sensitive nature of the information and will make sure that in dealing with it, no further breaches of confidentiality occur.

3. DEFINITION

Information which can be classified as "confidential" can broadly be grouped into the following areas:

- i. Personal information relating to Participants and ELECTED MEMBERS
- ii. Personal information relating to service users
- iii. Information relating to organisations
- iv. Business sensitive information relating to contracts or work programmes

A “breach” of confidentiality occurs when:

- i. A Participant and Elected Member with a need to know discloses information to a third party who does not have a need to know
- ii. A Participant and Elected Member who does not have a need to know gains access or attempts to gain access to sensitive and confidential information

4. MAINTENANCE OF CONFIDENTIALITY

- a) All Participants and ELECTED MEMBERS have a duty to treat participant, ELECTED MEMBER or service user information in the strictest confidence.
- b) Participants and ELECTED MEMBERS also have a duty to ensure that all information concerning participant, Elected Member and service users is used only for the purpose for which it was given.

5. PARTICIPANTS AND ELECTED MEMBERS MUST

- a) Be aware of their personal responsibility and undertake to abide by the policies and procedures of Birmingham LINK.
- b) Not access any record where there is no proper cause related to their work.
- c) Not disclose information where there is not a “need to know”.

6. NEED TO KNOW

- a) Sensitive information is only to be requested on a “need to know” basis. This means only when the information is necessary to provide a service or to manage the delivery effectively, and then only in the best interest of service users.

7. INFORMED CONSENT

- a) Information which is confidential and restricted will only be passed on where there is a clear need to know and where the expressed and informed consent has been obtained from the person whose information needs to be passed on.
- b) Informed consent should be sought every time there is a need for confidential information to be passed on to an authorised person.
- c) Wherever possible informed consent should be logged in writing as a form of contract.
- d) Confidential information will not be discussed on the telephone unless the identity of the caller is established. This will be checked when necessary, e.g. with call backs or security checks prior to the release of any information.

8. CIRCUMSTANCES IN WHICH INFORMATION CAN BE DISCLOSED

- i. With the individual's written consent for a particular purpose
 - ii. The information is required by law or under a court order
 - iii. In child protection investigations, cases or proceedings where it is considered that the information required is in the public and child's interest
 - iv. Child protection disclosures should always be discussed with the Senior Manager of the Host organisation
 - v. Where the disclosure can be justified for another reason. This is usually for the protection of the public and is likely to be in relation to the prevention and detection of a serious crime
- a) Difficult decisions to releasing information may require legal advice prior to disclosure. Where Participants and ELECTED MEMBERS are in any doubt they should always seek advice from the Senior Manager of the Host organisation.
 - b) Birmingham LINK must always be able to fully justify the release of confidential information.

9. CIRCUMSTANCES IN WHICH INFORMATION CANNOT BE DISCLOSED

- a) Where having been asked to state a view Participants, ELECTED MEMBERS and service users have expressed a wish that information should not be disclosed to any third party.
- b) Again, where failure to share information could result in harm to any member of the public or to the commission of a serious crime then the withholding of consent is deemed unreasonable and Participants and ELECTED MEMBERS are obliged to act on the information they hold by informing the appropriate authority or responding to requests for information from those authorities.

10. STORAGE OF DATA

- a) All documents that contain confidential or sensitive information should be stored securely using storage facilities that are fit for purpose.
- b) All information stored on electronic media, computers and mobile devices must be adequately protected.
- c) For further guidance please refer to the following Policy and Procedure document – Data Protection.

11. DISPOSAL OF INFORMATION

- a) All confidential data which is to be disposed of must be handled in a manner which maintains security. Such processes should be managed internally, using appropriate technologies.