

BIRMINGHAM LINK DATA PROTECTION POLICY

This policy document applies to your involvement with Birmingham LINK (“the Organisation”).

1. DATA PROTECTION PRINCIPLES

- a) The Organisation complies with the Data Protection Act 1998 and the principles of the Act, your personal data will be:
- i. Fairly and lawfully processed
 - ii. Processed for limited purposes and not in any way incompatible with those purposes
 - iii. Adequate, relevant and will not be excessive
 - iv. Accurate
 - v. Not kept for longer than necessary
 - vi. Processed in accordance with your individual rights
 - vii. Secure
 - viii. Not transferred to countries without adequate data protection

2. YOUR AGREEMENT

As part of your participation and elected membership of the Organisation, you agree to the collection and storage of your personal data within the scope of the Data Protection Act 1998.

3. YOUR PERSONAL DATA

- a) The Organisation only holds personal data directly relevant to your involvement. This data is collected as and when required from your involvement, such information includes, but is not limited to:
- i. Name
 - ii. Address
 - iii. Age
 - iv. Ethnicity
 - v. Gender
 - vi. Disability
 - vii. Faith
 - viii. Contact details

4. MAINTAINING RECORDS

- a) The Organisation will take all reasonable steps to ensure that personal data held by the Organisation is accurate and kept up to date. As a Participant or ELECTED MEMBER, you should always contact the Host organisation should your personal information change for any reason, for example a change of surname, home address or telephone number. Out of date information or information that is no longer required will be deleted by the Organisation on a regular basis.

5. SECURITY OF DATA

- a) The Organisation is committed to the secure storage and where undertaken the secure transmission of Participants and ELECTED MEMBERS personal data. Only trained members of staff within the Host organisation have access to such data. All such data is protected by physical security, such as locks and technical security, such as usernames and passwords to access computer records and data. Such data is only disclosed on a "need to know" basis. To further ensure the security of such records the Organisation reserves the right to monitor and keep detailed log file and computer data analysis of all accesses to Participant and ELECTED MEMBER's personal data.
- b) All Participants and ELECTED MEMBERS are reminded that unauthorised attempts to gain access to such data or accessing such data may constitute a criminal offence under the Data Protection Act 1998.

6. EXTERNAL DATA PROCESSING

- a) Where the Organisation uses the Host organisation or third parties to process data and provide services or administer schemes around such data the Host Organisation will take reasonable steps to ensure that such third parties have in place their own data protection policies.

b) EQUAL OPPORTUNITIES MONITORING

The Organisation may collect information relating to ethnic origin, sex or disability as part of an equal opportunities policy. The Organisation will ensure that any questionnaires relating to such information are accurate and that where possible the results will identify participation trends within the Organisation, and not identify individuals.

7. DATA TRANSFERS OUTSIDE THE EUROPEAN ECONOMIC AREA

If the Organisation transfers data outside the European Economic Area such data will only be transferred to countries deemed by the European Commission to provide adequate data protection or to countries, which are recognised "safe harbours" for such data. However, the Organisation may transfer data to other countries where the permission of the Participant and ELECTED MEMBER has been given.

8. DATA ACCESS AND DISCLOSURE

- a) All prospective, current or Participants or ELECTED MEMBERS have the right to request access to data directly relating to them, which is held by the Organisation. The Organisation is entitled to seek a fee of up to £10 to deal with each request. Furthermore the Organisation can request further information from the person making the request in order to provide accurate and relevant results and to check the identity of the person making the request. The Organisation seeks to provide such information within 40 days of receiving a request.

The Organisation will provide the person making the request with the following information:

- i. Whether they hold any information regarding them, and if they do:
 - ii. Descriptions of that information
 - iii. What it is used for.
 - iv. The type of third party Organisations it is passed to.
 - v. Provide a breakdown of any technical terms or codes.
- b) The information where reasonably possible will be provided in a hard copy in person on production of valid identification documents

9. EXTERNAL DISCLOSURE REQUESTS

- a) Where ELECTED MEMBERS or the Host organisation receive external requests for the disclosure of data the following guidelines should be observed:
- i. Verify the identity of the person requesting the information
 - ii. Be on the lookout for fraud or deception
 - iii. Seek a written request where possible
 - iv. Check any telephone numbers where an oral request is received
 - v. Inform the Senior Manager of the Host organisation if any request appears suspicious
 - vi. The Senior Manager should also be contacted where the party requesting the data states that disclosure is required by law
 - vii. Remember that a duty is owed to the individual whose data is to be disclosed, where possible seek their permission, unless doing so would alert them to a criminal investigation
 - viii. A record of all non-routine data disclosures should also be kept

10. OTHER DISCLOSURES

Where the Organisation wishes to disclose Participant or ELECTED MEMBER data for promotional, marketing or other business purposes, (for example incorporated into an advertisement or brochure) the consent of the Participant or ELECTED MEMBER should be sought in advance. The Participant or ELECTED MEMBER should also be told where the data will be published and how widely.

11. MONITORING

The Organisation will inform all ELECTED MEMBERS where monitoring is introduced or increased. The Organisation will take reasonable steps to ensure that ELECTED MEMBER's privacy and anonymity are preserved. The Organisation will take reasonable steps to ensure that specific details of personal conversations or correspondence are not accessed.

12. CCTV MONITORING

- a) The Organisation reserves the right to introduce or extend the use of CCTV within the Organisation's premises for security purposes. Where this occurs signs will be displayed on the premises to make it clear to staff and visitors that CCTV is being used.
- b) CCTV will only be used to monitoring activity on the Organisation's own premises.
- c) Recorded images will be stored securely; with only authorised Organisation members of staff and (where requested) the police will have access to them.
- d) Recorded images will only be retained for as long as necessary or where the police or courts require evidence.
- e) All CCTV equipment will be regularly inspected to ensure proper functioning.

13. CRIMINAL LIABILITY

Knowingly or recklessly disclosing the personal data of others without the express consent of the Organisation can constitute a criminal offence.

14. DATE OF IMPLEMENTATION

This policy is effective from February 2009 and shall not apply to any actions that occurred prior to this date.

15. QUESTIONS

If you have any questions regarding this policy document and how it applies to you, including how to request access to your personal data please consult the Senior Manager of the Host organisation.

16. ALTERATION OF THESE GUIDELINES

- a) These guidelines will be subject to change and updating. Any alterations will be communicated to you by the Senior Manager of the Host organisation.