

DATA PROTECTION POLICY

1 INTRODUCTION

Linlithgow Link is fully committed to full compliance with the requirements of the Data Protection Act 1998. Linlithgow Link will therefore follow procedures which aim to ensure that all employees and volunteers (collectively known as the data users) who have access to any personal data held by or on behalf of Linlithgow Link are fully aware of and abide by their duties under the Data Protection Act 1998.

2 STATEMENT OF POLICY

Linlithgow Link needs to collect and use information about people with whom it works in order to operate and carry out its functions. These may include prospective employees, clients and volunteers. This personal information must be handled and dealt with properly however it is collected, recorded and used and whether it is on paper, in computer records or recorded by other means.

Linlithgow Link regards the lawful and appropriate treatment of personal information as very important to its successful operation and essential to maintaining confidence between Linlithgow Link and those with whom it carries out its business. Linlithgow Link therefore fully endorses and adheres to the principles of the Data Protection Act 1998.

3 HANDLING PERSONAL AND SENSITIVE DATA

Linlithgow Link, through management and use of appropriate controls, monitoring and review:

- Use personal data in the most efficient and effective way to deliver better services
- Strive to collect and process only the data or information which is needed
- Use personal data for such purposes as described at the point of collection, or for purposes which are legally permitted
- Strive to ensure information is accurate
- Not keep information for longer than is necessary
- Securely destroy data which is no longer needed
- Take appropriate security measures to safeguard information
- Ensure that there is general information about individuals rights to access information

- Ensure that the rights of people about whom information is held can be fully exercised under the Data Protection Act 1998

These rights include:

- The right to access their own personal information within 40 days of request
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information regarded as wrong information
- Provide guidance and training for staff and volunteers
- Ensure that any breaches of the policy are dealt with appropriately

4 THE PRINCIPLES OF DATA PROTECTION

The Data Protection Act stipulates that anyone processing personal data must comply with 8 principles of good practice. These principles are legally enforceable. Summarised, the principles require that personal data:

- Shall be processed fairly and lawfully, in particular, shall not be processed unless specific conditions are met
- Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
- Shall be accurate and where necessary kept up to date
- Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
- Shall not be kept for longer than is necessary for that purpose or those purposes
- Shall be processed in accordance with the rights of data subjects under the Act
- Shall be kept secure, i.e. protected by an appropriate degree of security
- Shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of data protection

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and **sensitive personal data**.

Personal data is defined as data relating to a living individual who can be identified from:

- That data
- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual and any

indication of the intentions of the data controller, or any other person in respect of the individual

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin
- Political opinion
- Religious or other beliefs
- Trade Union Membership
- Physical or mental health or condition
- Sexual life
- Criminal proceedings or convictions

SEPTEMBER 2014

**Linlithgow Link (Voluntary Group) is a charity registered in Scotland No
SCO13502**