Data Protection Policy

Link UP London is committed to a policy of protecting the rights and privacy of individuals, including service users, staff, volunteers, colleagues and affiliates of the organisation, in accordance with the General Data Protection Regulations (GDPR) May 2018.

The GDPR contains provisions that Link UP London will need to be aware of as both data controllers and data processers, including provisions intended to enhance the protection of individuals personal data.

The organisation controls and processes the follow data:

- Information about service users – organisations, volunteers, staff and Link UP volunteers.
- The recruitment and payment of staff and volunteers
- The administration of programmes and courses
- Recording service users progress, attendance and conduct
- Collecting fees of any kind
- Images and information for marketing purposes

To comply with various legal obligations, including the obligations required by the General Data Protection Regulation (GDPR), Link UP London will ensure that all information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully without explicit consent or lawful obligation.

Compliance

This policy applies to all service users, staff, volunteers, colleagues and affiliates of the organisation. Any breach of this policy or of the Regulation itself will be considered an offence and will invoke the organisation's disciplinary procedure.

As a matter of best practice, other agencies and individuals working with Link UP London and who have access to personal information, will be expected to read and comply with this policy.

All staff who have access to any kind of personal data will be given access of all relevant policies and procedures during their induction process, including the Data Protection policy, and the operational procedures for handling personal data. All staff will be expected to adhere to all these policies and procedures. Volunteers will receive information about Data Protection as part of their induction.

This policy will be reviewed every 3 years and amended as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation.

General Data Protection Regulation (GDPR)

The GDPR regulates the controlling and processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

Data control

Link UP London will be the 'data controller' under the terms of the legislation –this means it is ultimately responsible for controlling the use and processing of the personal data. The organisation appoints a Data Protection Officer (DPO), currently the Communications Coordinator, who is available to address any concerns regarding the data held by organisation and how it is processed, held and used. Link UP's Directors will oversee this policy. The DPO is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the organisation.

Responsibility

Compliance with the legislation is the personal responsibility of all members of Link UP London who process personal information. Individuals who provide personal data to the organisation are responsible for ensuring that the information is accurate and up to date.

Data Protection principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles. More detailed guidance on how to comply with these principles can be found following this link to the ICO's website (www.ico.gov.uk)

In order to comply with its obligations, Link UP London undertakes to adhere to the eight principles:

P1. Process personal data fairly and lawfully

Link UP will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

P2. Purpose limitation

Link UP London will process data for the specific and lawful purpose for which it is collected and not further process the data in a manner incompatible with this purpose. The organisation will ensure that data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

P3. Data minimisation

Link UP London will ensure all data that is collected is adequate, relevant and limited to what is necessary in relation to the purposes. The organisation will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

P4. Keep personal data accurate and, where necessary, up to date

Link UP London will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the organisation if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the organisation to ensure that any notification regarding the change is noted and acted on.

P5. Storage limitation

Link UP London will not retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Link UP London will undertake a regular review of stored data and will dispose of unnecessary data in a manner that protects the rights and privacy of the individual involved. For example: secure electronic deletion, shredding and disposal of hard copy files as confidential waste.

P6. Process personal data in accordance with the rights of the data subject under the legislation

Individuals have various rights under the legislation including a right to:

- be told the nature of the information the organisation holds and any parties to whom this may be disclosed
- prevent processing likely to cause damage or distress
- prevent processing for purposes of direct marketing
- be informed about the mechanics of any automated decision-making process that will significantly affect them
- not have significant decisions that will affect them taken solely by automated process
- sue for compensation if they suffer damage by any contravention of the legislation
- take action to rectify, block, erase or destroy inaccurate data

If a data subject thinks that their data has been misused or that Link UP London has not kept it secure, they should contact Link UP London Data Protection Officer and tell them (follow Link UP London grievance policy and procedures). If the data subject is unhappy with their response or if they need any advice, they should contact the Information Commissioner's Office.

P7. Integrity and confidentiality

Link UP London will ensure data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties.

Link UP London will ensure that all personal data is accessible only to those who have a valid reason for using it. The organisation will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in a secure location:

- password protecting personal data held electronically
- archiving personal data which are then kept securely
- placing any PCs or terminals that show personal data so that they are not visible except to authorised staff
- ensuring that PC screens are not left unattended without a password protected screen-saver being used.
- appropriate back-up and disaster recovery solutions shall be in place.

Access to information on Sharepoint or Link UP London's databases are controlled by a password and only those needing access are given the password.

In addition, Link UP London will put in place appropriate measures for the deletion of personal data. Manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work.

Hard drives of redundant PCs will be wiped clean before disposal.

A log will be kept of the records destroyed. This policy also applies to staff and service users who process personal data 'off-site', e.g. when working at home.

As confidentiality applies to a much wider range of information than Data Protection, Link UP London includes confidentiality within its employment contracts, volunteer agreements and Code of Conduct policy.

Link UP London has a privacy statement for all staff, volunteers and affiliate members, setting out how their information will be used. This is shared with everyone on joining and is available on request. Staff and volunteers sign contracts in which confidentiality responsibilities are clearly laid out.

P8. Data Transfer outside the European Economic Area (EEA)

Link UP London will not transfer data to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals in relation to the processing of personal information.

CONSENT

Obtaining consent

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when Link UP London is processing any sensitive data, as defined by the legislation. The organisation understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Link UP London will ensure that data is collected within the boundaries defined within this policy. This applies to data that is collected in person (face to face or over the telephone), electronically or by completing a form. It applies to any location that is being used by staff, volunteers or contractors to deliver Link UP London related business.

When collecting data, Link UP London will ensure, wherever possible, that there is a fair processing notice in place and that the Individual:

- clearly understands why the information is needed
- understands what it will be used for and what the consequences are should the Individual decide not to give consent to processing (more relevant to sensitive information)
- understands who the data may be shared with and why
- has the option to agree to sharing the data
- grants explicit written or verbal consent to collect and share sensitive data wherever possible
- gives explicit consent to contact via email
- is competent enough to give consent and has given so freely without any duress.

Managing consent

The organisation will obtain separate photo consent on each occasion that a photograph is taken, with explicit information of the intended use of the data.

Created March 2021 to be reviewed again by March 2024