Agreed by Board: 7th August 2018
Review date: 7th August 2020

DATA PROTECTION AND SECURITY POLICY

EASY READ INTRODUCTION

Lewisham Speaking Up will keep information about you **safe** and will not talk to anyone or **share** your information unless **you say so**

We have to keep information about you so we can **help you** and do our advocacy work

We will only keep information about you if we **need to**

The law says we cannot share your information unless **you say** that we can.

The law is called **The Data Protection Act** and **GDPR** (General Data Protection Regulation)

The law says we must store your information in a **safe place**. We will store it on a **computer** with safe passwords or in a locked **cabinet**

The law says we have to **make changes** to your information if you **ask us to**

If **you decide** you do not want us to keep information about you anymore, we will **remove it**

If a mistake is made and your information is lost or stolen it is called a **breach**

If a breach happens we have to **tell you** and we have to tell an organisation called the **ICO** (Information Commissioner's Office)

DATA PROTECTION AND SECURITY POLICY

1. Introduction and purpose

Lewisham Speaking Up (LSU) is an organisation which respects the confidentiality of information given in the course of its business and will not disclose information to third parties or talk about clients or client organisations in any way that would compromise them or the organisation.

LSU holds information about what we do and who we work with. This includes information about participants we support, staff/volunteers working for the organisation and details of the Board of Trustees.

This policy provides guidelines for staff, volunteers and Board members to ensure that all such information remains confidential and is not disclosed to third parties.

This data protection policy ensures that LSU:

- Complies with data protection law and follows good practice
- Complies with GDPR (General Data Protection Regulation)
- Protects the rights of staff, participants and partners
- Is clear about how individuals information is stored and processed
- Protects itself from the risks of a data breach

LSU aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a Privacy Statement, setting out how data relating to individuals is used by the organisation.

2. Data Protection

LSU has identified that it is exempt from registering under the General Data Protection Regulation on the basis that information held is used to follow its charitable objectives.

To comply with the law, personal information must be collected, stored safely and not disclosed unlawfully. LSU will ensure that information will be:

- processed fairly and lawfully
- obtained only for specific, lawful purposes
- adequate, relevant and not excessive
- accurate and kept up to date
- not held for any longer than necessary
- processed in accordance with the rights of data subjects
- protected in appropriate ways
- not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

3. Implementing this policy

Everyone who works for or with LSU has some responsibility for ensuring data is collected, stored and handled appropriately.

All staff members that handle personal data, either for staff/volunteers, or participant records must ensure that the information is processed in line with this policy and data protection principles. . Failure to do so may lead to disciplinary action being taken against an employee and, in the case of serious breaches, dismissal.

The LSU Board is ultimately responsible for ensuring that LSU meets its legal obligations and the Data Protection staff lead, Ilse de Kock, Administration Officer is responsible for:

- Keeping the board updated about data protection and GDPR responsibilities, risks and issues.

- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection/GDPR training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.
- Dealing with requests from individuals to see the data LSU holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Ensuring passwords are regularly changed (monthly)
- Evaluating any third-party services the company is considering using to store or process data. For instance, cloud computing services.

The Director as Data Controller is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

4. Data Processing

The processing of personal data (including its storage) must be done under one of the legal bases below. If you are processing personal data, you must document the reason why you need it and which of these legal bases it falls under.
These are:

- Consent (that is specific, freely given, and easily withdrawn) of the data subject

- Contractual obligations
- Legal obligations
- Protecting the subject's vital interests
- Statutory obligations
- "Legitimate interest"

The most common for LSU are likely to be consent, contractual and legal obligations, or "legitimate interest". This means we need to process the data for our business to function and to deliver our charitable objectives, and we must do so fairly and transparently.

5. Protecting our Data

This policy describes how LSU collects, handles and stores personal information in line with The Data Protection Act 1998. These rules apply regardless of whether data is stored electronically, on paper or on other materials.

All staff are expected to take great care to ensure they are protecting LSU's data:
Access to our IT systems is protected by the use of passwords. System access passwords must:

- Be complex to ensure they are not easy to guess
- Be changed regularly
- Not be written down or shared with others.

When sending documents containing personal information, staff must always use a password to protect the document. The password should be sent separately to the recipient, ideally via another medium (such as text message, phone call, or instant messaging service). Where you have a need to send personal data on a regular basis, it is acceptable to agree a regular password with the recipient.

If you use extractable media, such as a USB memory stick, so store data, you must ensure it is encrypted and stored in a secure fashion.

Staff must not leave information on display when they are away from their desks, unless it is already in the public domain. There are frequent visitors to the office who should not have access to such information.

At the end of each day or during prolonged periods away from the desk, any confidential information should be stored in locked cabinets.

Similarly, care should be taken to ensure information displayed on screen is not visible to those who are not authorised to access it. If you are viewing confidential information, be sure to check who is around you. When away from your desk, ensure you lock your PC (done by pressing either the windows key and "L", or by pressing control, alt, and delete and selecting the option to lock your screen.

6. Handling Personal Data

Staff must ensure they are familiar with their obligations under data protection legislation. LSU will provide training to staff from time to time, but there are many good free sources of information. The Information Commissioner's Office has a useful online guide to data protection on its website, here: https://ico.org.uk/for-organisations/guide-to-data-protection/

The people we hold data about are known as data subjects. They have a number of rights as data subjects. Under current (GDPR) legislation, these are defined as:

i. The right to be informed
ii. The right of access
iii. The right to rectification
iv. The right to erasure
v. The right to restrict processing
vi. The right to data portability
vii. The right to object

viii. Rights in relation to automated decision making and profiling.

Staff should bear these rights in mind when dealing with data subjects. In particular, the right of access has been broadened by the recent changes in legislation and all staff should be aware of how to handle a subject access request as set out in the following section.

7. Subject Access Requests

All individuals who are the subject of personal data held by LSU are entitled to:

- Ask what information the organisation holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the organisation requesting this information, this is called a subject access request. They can do this verbally or in writing and they do not have to state that it is a subject access request.

The person receiving the request should record the request and promptly inform the Director/ Data Controller.

The data controller will aim to provide the relevant data within 14 days and will always verify the identity of anyone making a subject access request before handing over any information. The information must be provided in a commonly accessible format.

8. Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal information to be disclosed to the following without the consent of the data subject:

- Law enforcement agencies (Section 29 requests)
- Other organisations such as Health & Safety Executive
- Official Receiver
- Solicitors acting on a client's behalf or a Solicitor asking for another's data.
- Also local authorities or public bodies acting under authorised powers.

Under these circumstances, LSU will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the Board where necessary.