Agreed by Board: 22nd September 2020
Review date: 22nd September 2022

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/students working for the organisation and details of the Board of Trustees.

This policy provides guidelines for staff, volunteers, students 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, volunteers, students and partners
- Is clear about how an individual's 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 organisation has relevant Privacy Notices for beneficiaries/friends/partners/stakeholders; volunteers/students; and staff 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 (no longer than 6 years)
- 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 who handle personal data, either for staff/volunteers/students, 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.
- Arranging regular checks and scans to ensure security hardware and software is functioning properly.
- Ensuring passwords are regularly changed (quarterly)
- 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 – *for example, permission letters on acceptance of employment, volunteering, or agreement to receiving 1-2-1 advocacy*
- 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 GDPR. 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. See Appendix A for our Risk Management Strategy.

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. There are also free sources of information available. 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:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. 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.

Appendix A

LSU Risk Management Strategy

- An Internet facing firewall to prevent outside penetration of the organisations network. Policies allow mail to be delivered into the mail server from a specific set of addresses (our external spam filter) but no other access is allowed. This firewall also maintains a list that prevents access to malicious sites on the WWW.
- Spam filtering. All our mail passes through a spam filter which looks for unsolicited mail, malicious software and dangerous links. All incoming mail is routed through Microsoft's firewall and anti-spam filters before reaching the Office 365 mail server.
- Local firewalling. All our computers are individually protected by a firewall. This prevents problem software proliferating through the network and unauthorised access from one machine to another e.g. only the IT Manager can remotely connect to a LSU computer or laptop.
- Local anti-virus to prevent any malicious software getting through the firewall or spam filters or be brought in by other means. Every machine in the Company has anti-virus software installed which is constantly updated via a server on the network. This software also maintains a web blacklist to prevent access to malicious sites. The Windows anti-virus system is regularly updated by Microsoft.
- File access controls. Access to data on the servers is controlled based on need. Management authority is required before any changes of access are made.
- Encryption. All company emails sharing personal data are encrypted when the recipient supports encryption.
- Filing cabinets. Data kept in employee's personnel files are stored in lockable cabinets.
- Archive room. Data kept at the end of an employee relationship is stored in a locked archive room with restricted access.
- IT Policy. This policy is to ensure that all information technology users within the organisation or its networks comply with rules and guidelines related to the security of the information stored

digitally at any point in the network or within the organisations boundaries of authority.

- Social Media Policy. This policy is aimed to educate employees and minimise risks when using social media which can impact the organisation and employees.
- 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 via another medium (such as text message, phone call, or instant messaging service). Where personal data is sent on a regular basis, it is acceptable to agree a regular password with the recipient.
- If using extractable media, such as a USB memory stick, to store data, 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. This is to prevent visitors to the office from accessing such information.
- Similarly, care should be taken to ensure information displayed on screen is not visible to those who are not authorised to access it. When away from your desk, staff must lock their PC (windows key and "L", or control, alt and delete and selecting the option to lock the screen).
- At the end of each day or during prolonged periods away from the desk, any confidential information should be stored in locked cabinets.

Appendix B

Response Plan

The purpose of this plan is to have effective procedures in place to deal with potential security incidents compliant with the General Data Protection Regulation (GDPR). This includes the implementation of recovery procedures including, where necessary, damage limitation measures.

Data Breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes.

Steps taken to prevent breaches:

1. Lewisham Speaking Up has a Data Controller and a Data Protection staff lead in place who has strategic responsibility for Data Protection and who has responsibility for information governance matters including compliance with data protection rules.
2. Policies and procedures for breach prevention have been put in place e.g. physical files policy.
3. Privacy notices have been developed to ensure that staff, participants, volunteers, students and stakeholders are made aware of GDPR and its implications for them.
4. A training plan is in place. All staff and members must complete an online training module which informs them of GDPR.

Appendix B

Steps taken in event of possible breach:

Under the GDPR, the organisation is obliged to notify the Information Commissioner's Office (ICO) of breaches which have a risk of affecting the rights and freedoms of individuals within 72 hours. The purpose of immediate notification is to encourage the data controller to act promptly, contain the breach and if possible, recover the personal data.

Where a breach has been intimated to the organisation by way of a complaint this should be dealt with in the normal manner i.e. in line with the organisation's complaints process but in addition complainers should be advised of their right to raise the issue with the ICO.

A. Notification to data controller and data protection staff lead

1. As soon as a member of staff, a volunteer or a student becomes aware of a security incident or possible breach, they should inform their line manager immediately who in turn must inform the Data Protection staff lead and the Data Controller. Immediate notification is required due to the requirement to notify the ICO of a breach within 72 hours of having a reasonable degree of certainty that an incident has occurred. (See D).

2. There are three types of data protection breach:

   Confidentiality breach: where there is an unauthorised or accidental disclosure of, or access to, personal data.

   Availability breach: where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

   Integrity breach: where there is an unauthorised or accidental alteration of personal data.

B. Investigation by Data Controller

1. The Data Controller must carry out an urgent investigation to establish the facts so that an informed decision can be made as to whether rights and freedoms have been breached and ICO notification is required. The breach checklist is a useful guide to the facts that need to be established and should be completed as a matter of urgency.

2. The Data Controller should check any relevant Data Privacy Impact Assessment which may assist in determining the effect of the breach on the person whose information has been lost, disclosed etc.

3. Once the initial investigation is complete, it needs to be ascertained whether the completion of the ICO notification form is required for submission.

   It is understood that it may not be possible to collate all the information immediately but a referral to the ICO must be made within 72 hours of referable breaches. Thereafter, the investigation can be continued as required and further information provided to the Data Controller when known.

C. Data Controller determination

The Data Controller needs to make an objective assessment of the risk and assess whether the rights and freedoms of an individual have been breached and ICO notification is required. Consideration of the likelihood and severity of the risk and circumstances are required e.g. take into account the special characteristics of the individual.

D. Notification to ICO and other relevant persons

1. ICO

The notification form will be submitted to the ICO if the Data Controller determines that there has been a risk to the individual's rights and freedoms. As a minimum, the following information must be provided:

- Description of nature of the breach i.e. categories of individual/information;
- and numbers affected;
- Name and contact details of Data Controller;
- Likely consequences of breach;
- Description of measures taken.

Notification to the ICO can be carried out in phases if it is not possible to collate all the information within the 72-hour period. If it is not possible to notify within 72 hours, reasons for the delay must be provided. Further investigations may result in notification to the ICO that there has not been a breach.

2. Data Subject

Urgent consideration must be given as to whether the data subject should be informed. Notification is only required where there is a high risk to the individual's rights and freedoms. Therefore, the threshold is higher for intimation to individuals than it is for notification to the ICO. Such intimation must be made as soon as reasonably feasible.

The Data Controller will decide on the best means of contacting the individual. The following information should be provided to the individual:

- Description of nature of breach;
- Name and contact details of Data Controller;
- Description of likely consequences of breach;
- Description of measures taken;
- Advice to help the individual protect themselves from effects of the breach where appropriate.

Individuals should also be advised of their right to refer the matter to the ICO where they are not satisfied with the organisation's response to the breach. How to contact the ICO.

3. Police

A breach of GDPR could be a criminal offence. The DPO will determine if the matter needs to be referred to the Police.

4. Board of Trustees

The Data Controller should consult with the Board of Trustees to see if disciplinary action is appropriate.

5. The Charity Commission

The Data Controller should consult with the Board of Trustees to consider whether a serious incident report needs to be made to the Charity Commission. The Charity Commission cites a data protection breach that has occurred and has been reported to the ICO as an example of when a charity should submit a report.

E. Take Action

1. The Data Controller will liaise with other services, as appropriate, on the immediate steps, if any, required to ensure damage limitation e.g. recovery action by IT. It may be that urgent action must be taken whilst the investigation is ongoing (See B).

2. Having considered all the facts the Data Controller must decide what remedial measures are necessary e.g. review of existing policies or procedures; new policies or procedures or if additional or modified training is required. An action plan will be put in place when deemed necessary.

3. Any necessary measures will be undertaken

F. ICO determination

Data Controller and Data Protection staff lead to review ICO response and agree any recommended actions (See E).

G. Register

1. The Data Controller will complete the organisation's register of breaches. Under the GDPR, the organisation is required to maintain a register with details of the breach, effects and consequences, remedial action and reasoning for decisions taken. This register is kept on the Director's SharePoint site and is restricted to viewing by the Director and Data Protection staff lead.

2. Details of the entry on the Register will be made available to the Board of Trustees as a means of sharing lessons learnt and to improve awareness and best practice.

Further guidance on data protection breaches is available at ICO guidance.