

**Data Protection Policy and Procedures**

# Introduction

SLRA is committed to a policy of protecting the rights and privacy of individuals. SLRA needs to collect and use certain types of Data in order to carry out our work. This personal information must be collected and dealt with appropriately.

The Data Protection Act 1998 (DPA) governs the use of information about people (personal data) which will be superseded by the General Data Protection Regulation (GDPR) May 2018. Personal data can be held on computer or in a manual file, and includes email, minutes of meetings, and photographs. SLRA will remain the Data Controller for the information held. SLRA staff and volunteers will be personally responsible for processing and using personal information in accordance with the GDPR.

Trustees, staff, and volunteers of SLRA who have access to personal information, will be expected to read and comply with this policy.

# Purpose

The purpose of this policy is to set out SLRA’s commitment and procedures for protecting personal data.

SLRA regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

1. We want to collect limited relevant personal information of clients in order to provide appropriate and accessible support.
2. We want to use (1) to contact clients about the support we are providing and to update them with relevant information.
3. We want to use (1) to refer clients to appropriate services and to make enquiries on behalf of our clients to appropriate services.
4. We want to collect personal information from our referral partners and volunteers in order for our service to ensure good communication.
5. We want to maintain a list of people who have donated to us before, so that we can contact them to ask them to do so again.
6. We want to claim gift aid on a person’s donations.
7. We want to maintain accurate records of clients in order to anonymise data to use in funding applications and publicity.
8. We want to use the limited personal data we collect and store for 5 years before anonymising for long term use in order to assess the impact of our services.
9. We want to maintain contact information for anyone who has volunteered for SLRA so we can contact them about future volunteering opportunities.
10. We want to keep our volunteer, client and referrer database information up to date.

# The GDPR

In line with the GDPR principles (Article 5), SLRA will ensure that personal data will:

* Be obtained fairly and lawfully and shall not be processed unless certain conditions are met
* Be obtained for a specific and lawful purpose
* Be adequate, relevant but not excessive
* Be accurate and kept up to date
* Not be held longer than necessary
* Be processed in accordance with the rights of data subjects
* Be subject to appropriate security measures
* Not to be transferred outside the European Economic Area (EEA)

The definition of ‘Processing’ is obtaining, using, holding, amending, disclosing, destroying and deleting personal data. This includes paper based personal data as well as that kept on computer.

The Personal Data Guardianship Code suggests five key principles of good data governance on which best practice is based. SLRA will seek to abide by this code in relation to all the personal data it processes, i.e.

* **Accountability:** those handling personal data follow publicised data principles to help gain public trust and safeguard personal data.
* **Visibility:** Data subjects should have access to the information about themselves that an organisation holds. This includes the right to have incorrect personal data corrected and to know who has had access to this data.
* **Consent:** The collection and use of personal data must be fair and lawful. Personal data should only be used for the purposes agreed by the data subject. If personal data is to be shared with a third party or used for another purpose, the data subject’s consent should be explicitly obtained.
* **Access:** Everyone should have the right to know the roles and groups of people within an organisation who have access to their personal data and who has used this data.
* **Stewardship:** Those collecting personal data have a duty of care to protect this data throughout the data life span.

# Type of Information Processed

SLRA processes the following personal information (information that allows a person to be identified):

* Volunteer and donor name, address, email and contact number
* Referrer name, email address and contact number
* Client name, full address, postcode, gender, ethnicity, employment status, housing status, immigration status, sex and age of children under 18 years..
* Information required by HMRC in relation to financial donations subject to Gift Aid.

Personal information is collected using a paper registration form which is uploaded directly to SLRA’s client database at which point the paper copy is destroyed. If paper requests of referrals or volunteer applications are received they are uploaded to the client database upon which the paper copy is destroyed.

Staff data including personal and financial records are only available to the Director, Trustee Treasurer and pay roll.

Groups of people within the organisation who will process personal information are:

* Trustees, staff, reception volunteers, advice and casework volunteers.

# Applying the GDPR within SLRA

Whilst access to personal information is limited to the aforementioned staff and volunteers at SLRA, staff or volunteers may undertake additional tasks which involve the collection of personal details from members of the public.

In such circumstances we will let people know why we are collecting their data and it is our responsibility to ensure the data is only used for this purpose.

# Correcting data

Individuals have a right to have data corrected if it is wrong, to prevent use which is causing them damage or distress or to stop marketing information being sent to them.

# Responsibilities

SLRA is the Data Controller under the GDPR, and is legally responsible for complying with the GDPR, which means that it determines what purposes personal information held will be used for.

The Board of Trustees will take into account legal requirements and ensure that it is properly implemented, and will, through appropriate management, strict application of criteria and controls:

* + Observe fully conditions regarding the fair collection and use of information,
  + Meet its legal obligations to specify the purposes for which information is used,
  + Collect and process appropriate information and only to the extent that it is needed to fulfil its operational needs or to comply with any legal requirements,
  + Ensure the quality of information used,
  + Ensure that the rights of people about whom information is held, can be fully exercised under the GDPR. These include:
    - The right to be informed that processing is being undertaken
    - The right of access to one’s personal information
    - The right to prevent processing in certain circumstances and
    - The right to correct, rectify, block or erase information which is regarded as wrong information
  + Take appropriate technical and organisational security measures to safeguard personal information,
  + Ensure that personal information is not transferred abroad without suitable safeguards,
  + Treat people justly and fairly whatever their age, religion, disability, gender, sexuality or ethnicity when dealing with requests for information,
* Set out clear procedures for responding to requests for information

The Data Protection Officer on the Board of Trustees is:

The Data Protection Officer is the Director

Name: Celia Sands

Contact Details: [celia@slr-a.org.uk](mailto:celia@slr-a.org.uk)

The Data Protection Officer(s) will be responsible for ensuring that the policy is implemented and will have overall responsibility for:

* + Ensuring that everyone processing personal information understands that they are contractually responsible for following good data protection practice
  + Ensuring that everyone processing personal information is appropriately trained to do so.
  + Ensuring that everyone processing personal information is appropriately supervised
  + Ensuring that anybody wanting to make enquiries about handling personal information knows what to do
  + Dealing promptly and courteously with any enquiries about handling personal information
  + Describing clearly how SLRA handles personal information
  + Regular review and audit of the ways SLRA holds, manages and uses personal information
  + Regular assessment and evaluation of SLRA’s methods and performance in relation to handling personal information
  + Ensuring that all staff and volunteers are aware that a breach of the rules and procedures identified in this policy may lead to action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the GDPR.

In case of any queries or questions in relation to this policy please contact the Data Protection Officer.

# Training

Training and awareness raising about the GDPR and how it is followed in this organisation will take the following forms:

On induction:

All SLRA staff, trustees and volunteers are given a copy of our data protection policy and asked to sign the Confidentiality and Data Protection Agreement to show they have read and understood the policy. Specific induction is given regarding staff, trustee and volunteer roles that deal with personal data. Only staff and key volunteers ( Reception, casework and advice volunteers) have access to the online database.

General training / awareness raising: reminders of data protection are included in volunteer and staff supervision sessions and any changes or amendments to the GDPR and/or this policy will be communicated to relevant staff, trustees and volunteers.

Further training is available to trustees and staff through outside agencies where necessary and training logs are kept.

# Data collection

Before personal information is collected, we will consider:

* What information we need in order to deliver our service efficiently
* What information we need in order to show the impact of our service
* How long we will keep the information on record -
* We will keep data on clients for a maximum of 5 years from the client’s last use of our service.
* We will keep volunteer data for 1 year after their last contact with us, then it will be deleted.
* We will keep data on Gift Aid declarations for 6 years, in accordance with HMRC regulations.
* Anonymised data and aggregate totals will be maintained beyond the destruction of individual records so we can assess the impact of our services.

We will inform people whose information is gathered about the following:

* That we need key information in order to deliver our service
* That their information will be recorded in our Client Database, which is only accessed by staff and key volunteers and is password protected.
* That by ticking the box on the client registration form, they consent to SLRA using their anonymised data.
* That by ticking the box on the referral form, they consent to being contacted in order for us to complete our service.
* That staff will have relevant financial and personal information kept in the HR files in order to enable SLRA to meet legal and contractual obligations.

# Data Security

The organisation will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. The following measures will be taken:

* All referrals are received on a paper referral form which are kept securely in the SLRA office until personal information is uploaded to our online database. Paper referral forms are then destroyed.
* Once entered into the online database all information is only accessible to key staff and volunteers using a personal log in and password.
* Volunteers are sometimes tasked with collecting the above data from clients and recording this on a paper referral form. All volunteers are specifically told in their induction and reminded in supervision that all paper copies of referral documents should be held securely until taken to the SLRA office given and given to the Office Administrator at the end of each session. The Office Administrator will shred all referral forms once they have been uploaded to the online database.
* Information about volunteers submitted on paper copies of volunteer registration forms and agreements are destroyed as soon as volunteer information is uploaded to the online database.
* Electronic copies of DBS Certificates are kept securely and password protected.
* SLRA will use our best efforts to ensure that any outside agencies or contractors used to process data (such as payroll, fundraising etc.) also comply to the law and will adhere to the GDPR regulations.

# Existing Records

SLRA intends to use the “legitimate interest” principle of the GDPR in relation to information about volunteers and donors which was collected and stored before the date of this policy. Appendix 1 details the circumstances in which legitimate interest will be applied.

# Data Breach

Any unauthorised disclosure of personal data to a third party by an employee may result in disciplinary action being taken.

The trustees are accountable for compliance of this policy. A trustee could be personally liable for any penalty arising from a breach that they themself have made.

Any unauthorised disclosure made by a volunteer may result in the termination of the volunteering agreement.

If a volunteer or member of staff is made aware of a data breach they should notify the Director who will then inform the Trustee responsible for data protection.

Any serious data breaches or data loss will be reported to the Information Commissioners Office and the Charity Commission. This includes:

* Charity data that has been accessed and/or deleted by an unknown person.
* A charity device, containing personal details of beneficiaries or staff, has been stolen or gone missing and has been reported to the police;
* Charity funds lost due to an online or telephone ‘phishing scam’, where staff or trustees were conned into giving out bank account details;
* A Data Protection Act breach has occurred and been reported to the ICO.

# Data Subject Access Requests

Anyone whose personal information we process has the right to know:

* What information we hold and process on them
* How to gain access to this information
* How to keep it up to date
* What we are doing to comply with the Act.

They also have the right to prevent processing of their personal data in some circumstances and the right to correct, rectify, block or erase information regarded as wrong.

Individuals have a right under the Act to access certain personal data being kept about them on computer, online database and certain files. Any person wishing to exercise this right should apply in writing to Celia Sands ( Celia@slr-a.org.uk)

The following information will be required before access is granted:

* Full name and contact details of the person making the request
* Relationship with the organisation and applicable timescales

We may also require proof of identity before access is granted. The following forms of ID will be required: passport or birth certificate.

Queries about handling personal information will be dealt with swiftly and politely.

We will aim to comply with requests for access to personal information as soon as possible, but will ensure it is provided within the 28 days from receiving the written request required by the GDPR .

# Disclosure

SLRA may need to share data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Data Subject will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows SLRA to disclose data (including sensitive data) without the data subject’s consent.

These are:

* 1. Carrying out a legal duty or as authorised by the Secretary of State
  2. Protecting vital interests of a Data Subject or other person
  3. The Data Subject has already made the information public
  4. Conducting any legal proceedings, obtaining legal advice or defending any legal rights
  5. Monitoring for equal opportunities purposes – i.e. race, disability or religion
  6. Providing a confidential service where the Data Subject’s consent cannot be obtained or where it is reasonable to proceed without consent: e.g. a safeguarding concern for the welfare of the child or vulnerable adult

SLRA regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we work.

# Risk Management

The consequences of breaching Data Protection can cause harm or distress to clients if their information is released to inappropriate people, or they could be denied a service to which they are entitled. Volunteers should be aware that they can be personally liable if they use clients’ personal data inappropriately. This policy is designed to minimise the risks and to ensure that the reputation of SLRA is not damaged through inappropriate or unauthorised access and sharing.

# Further information

If members of the public/or stakeholders have specific questions about information security and data protection in relation to SLRA please contact the Data Protection Officer.

The Information Commissioner’s website (www.ico.gov.uk) is another source of useful information.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Date Implemented:  May 2018 | Future Review Dates | | | | | |
|  |  |  |  |  |  |
| Last Date reviewed/Revised |  |  |  |  |  |  |
| Date approved By Trustees |  |  |  |  |  |  |

**Appendix 1: SLRA GDPR Approaches**

**Background and Definitions**

*CONSENT*

*Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the*

*Act gives effect) defines an individual’s consent as:*

*…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.*

Under the GDRP, organisations using consent as the basis for contact or data processing, will need to actively collect and then maintain consents (opt-ins) from existing and new contacts in order to store information, or before any contact can be made (using personal data). The bar is set very high on the quality of this consent.

*LEGITIMATE INTEREST*

*GDPR presents legitimate interest as a valid condition for processing as follows:*

*“where processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.”*

Organisations using legitimate interest as the basis for processing data will need to be able to demonstrate that they have balanced the rights of the individual data subject with their own interests. They will need to record and explain the rationale for using legitimate interest and they need to be aware that the data subject can challenge.

Contacting all individuals who we already hold data on to collect permission could lead to a significant reduction in numbers of people on our databases. Not everyone will respond and of those that do, tick a consent box – even if they are actively in contact with SLRA. Harvesting and maintaining permissions could quickly become the major preoccupation of operating teams.

Legitimate interest is a simpler approach and recent guidance from the Information Commissioner’s Office (ICO) suggests they now consider this route is likely to be chosen by charities in many cases. However, the charity needs to specify and record the grounds on which it believes legitimate interest applies in each case. Organisations can also not rely on consent and legitimate interest for the same set of data, i.e., if a group of individuals are contacted to request consent but consent is not given by some, we could not then retain their information under legitimate interest.

**Proposed Approaches for SLRA**

Our updated Data Protection Policy outlines the personal information we collect on various groups that come into contact with our charity, why this is collected and how and why it is held. We have updated all the forms we use to collect this information to contain a robust set of consents around storing data and opt-ins for future contact for relevant reasons depending on the group of people using the form. Given consents will be recorded and stored securely.

To judge which route should apply, and to enable us to articulate these to others, we set out to establish some principles.

* We believe we have a legitimate interest to contact volunteers and referrers which enable us to operate.
* We would balance the interests of volunteers and referrers with our need to operate.
* Where we are using legitimate interest we would ensure we are staying within the realms of what people might expect.
* We would use legitimate interest as a basis to contact engaged volunteers and referrers with materials consistent with their current behaviour.
* We would use legitimate interest to contact existing volunteers and referrers with newsletters and through this route invite further participation via consent.
* We would use consent for all new contact clients, volunteers and referrers.

**Fundraising**

We do not currently have any (or very few) financial donors on a regular giving scheme, and as such do not have a large financial donor database who we would contact about and future fundraising campaigns. If this is something we decide to pursue in the future, we should revisit this policy. Many other charities are relying on legitimate interest for contact relating to fundraising.

**Action Plan**

|  |  |  |
| --- | --- | --- |
| **Group** | **Proposed Approach** | **Action Required** |
| Existing Volunteers | Legitimate interest to hold their information as charity needs to be able to contact them to operate. Not harming rights of individuals as contact is in line with reason individuals originally provided data.  Inform individuals that they will be kept on our database and give them the option to opt-out. | Send email to existing volunteers on our data base (legitimate interest) including link to new policy and notification of right to have data removed and no longer receive correspondence: Email to be sent May 2018 |
| New Volunteers | Collect consents (data retention and future contact) at point of registration and store securely on online database. | Volunteer registration form to be updated with new opt-in consents.  Staff to email consents to individuals contacting us not using standard forms. |
| Existing Clients | All clients for whom data currently held on online database have previously provided consent (data retention and future contact)  Hold anonymised data in line with policy. | Review online database security regularly. |
| New clients | Collect consents (data retention and future contact) at point of registration and store securely. | Paper and online registration form to be regularly reviewed.  Staff to email consents to individuals contacting us not using standard forms. |
| Donors - financial | We retain the information we are required to relating to Gift Aid. This is in the legitimate interest of the charity to allow us to comply with regulations.  If we wanted to use this information to contact donors about future giving, we could use legitimate interest but we should revisit this at the time. |  |

## Checklist at May 25th 2018

### Asking for consent

* We have checked that consent is the most appropriate lawful basis for processing.
* We have made the request for consent prominent and separate from our terms and conditions.
* We ask people to positively opt in.
* We don’t use pre-ticked boxes or any other type of default consent.
* We use clear, plain language that is easy to understand.
* We specify why we want the data and what we’re going to do with it.
* We give separate distinct (‘granular’) options to consent separately to different purposes and types of processing.
* We name our organisation and any third party controllers who will be relying on the consent.
* We tell individuals they can withdraw their consent.
* We ensure that individuals can refuse to consent without detriment.
* We avoid making consent a precondition of a service.
* We have age-verification measures (and parental-consent measures for younger children) in place.

### Recording consent

* We keep a record of when and how we got consent from the individual.
* We keep a record of exactly what they were told at the time.

### Managing consent

* We regularly review consents to check that the relationship, the processing and the purposes have not changed.
* We have processes in place to refresh consent at appropriate intervals, including any parental consents.
* We consider using privacy dashboards or other preference-management tools as a matter of good practice.
* We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.
* We act on withdrawals of consent as soon as we can.
* We don’t penalise individuals who wish to withdraw consent