Data Protection Policy 2017-2018
(incl. Key Procedures)

A. The scope of this policy

SPPA needs to keep certain information on its Members, employees, volunteers, service users and trustees to carry out its day to day operations, to meet its objectives and to comply with legal obligations.

The organisation is committed to ensuring any personal data will be dealt with in line with the Data Protection Act 1998. To comply with the law, personal information will be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

The aim of this policy is to ensure that everyone handling personal data is fully aware of the requirements and acts in accordance with data protection procedures. This document also highlights key data protection procedures within the organisation.

This policy covers all employed staff, trustees, volunteers, Members & users of its services.

B. Contents

1. Definitions

In line with the Data Protection Act 1998 principles, SPPA 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 some 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. The organisation 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 and in accordance with the DPA's eight data protection principles. 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.

2. Type of information processed

SPPA processes the following personal information:

- Name & Date of Birth
- Addresses – both personal & professional
- Email and Phone Numbers
- Members and event attendees bank details (for 12 months or longer where repeat subscription or donation)

Personal information is kept in the following forms:

- Electronic – email, database, spreadsheet, letter
- Received post – letters, administration, newsletters
- Payroll, bank account

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

- Employees
- Trustees
- Volunteers

3. Notification

The needs we have for processing personal data are recorded on the public register maintained by the Information Commissioner. We notify and renew our notification on an annual basis as the law requires.

If there are any interim changes, these will be notified to the Information Commissioner within 28 days.

The name of the Data Controller within our organisation as specified in our notification to the Information Commissioner is Carla Aylmore.

4. Responsibilities

Under the Data Protection Guardianship Code, overall responsibility for personal data in a not for profit organisation rests with the governing body. In the case of SPPA this is the Board of Trustees.

The governing body delegates tasks to the Data Controller. The Data Controller is responsible for:

- understanding and communicating obligations under the Act
- identifying potential problem areas or risks
- producing clear and effective procedures
- notifying and annually renewing notification to the Information Commissioner, plus notifying of any relevant interim changes

All employed staff, trustees and volunteers who process personal information must ensure they not only understand but also act in line with this policy and the data protection principles.

Breach of this policy will result in suspension pending further investigation and may lead to dismissal for employed staff, trustees and volunteers.

5. Policy Implementation

To meet our responsibilities staff, volunteers and trustees will:

- Ensure any personal data is collected in a fair and lawful way;
- Explain why it is needed at the start;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure it is kept safely;
- Ensure the rights people have in relation to their personal data can be exercised

We will ensure that:

- Everyone managing and handling personal information is trained to do so.
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, volunteer or service user, knows what to do;
- Any disclosure of personal data will be in line with our procedures.
- Queries about handling personal information will be dealt with swiftly and politely.

6. Training

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

On induction:

- All staff, volunteers and Trustees will receive copies of this policy and other relevant guidelines relating to the Act
- Will be required to sign to acknowledge their receipt & understanding of the policy
- Where appropriate, will be provided with security information (passwords, keys etc) and be required to acknowledge the importance of retaining privacy and security for files, documents, computer systems etc

General training/ awareness raising:

- All staff, volunteers and Trustees will receive bi-annual reminders and/or updates relating to the policy

7. Gathering and checking information

Before personal information is collected, we will consider:

- Purpose of data collection
- Details necessary to fulfil purpose
- Length of time information will be retained
- Format of collection and retention
- Protection method for data

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

- Why information is being gathered
- What information will be used for
- Who will have access to information (including Third Parties)
- Length of time information will be retained
- How information will be retained and methods of protection to be used

We will take the following measures to ensure that personal information kept is accurate:

- Sending a request to individuals, asking them to check and confirm initial data is correct
- Forwarding an annual request, for as long as the data is held, asking individuals to confirm data held is accurate
- Where no response is received to the data check request, an individuals' data will be removed after 12 months

Personal sensitive information will not be used apart from the exact purpose for which permission was given.

8. 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:

- Minimising the number of individuals with access to personal data

- Using password protection and encryption when forwarding, receiving or retaining data on computer systems
- Using lockable cupboards/drawers to store paper versions of data collected
- Restricting access to files containing personal data (both paper and electronic)
- Not allowing data to be taken off site (whether as hard copy or electronic versions)
- Backing up to secure servers off site any data collected and retained
- Using password protection when sending data electronically

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

Any unauthorised disclosure of personal data to a third party by a volunteer or trustee may result in their removal from the organisation with immediate effect.

9. 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 and certain files. Any person wishing to exercise this right should apply in writing to Lewis Smith, SPPA Project Officer.

We will make a charge of £10 on each occasion access is requested.

The following information will be required before access is granted:

- Completion of Data Access Form
- Provision of ID

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

- Identification – passport, photo driving licence, country ID etc
- Proof of Address – Bank statement, insurance documents, amenity bill (not mobile phone); must be no older than 6 months

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 40 days required by the Act from receiving the written request and relevant fee.

10. Review

This policy will be reviewed at intervals of 2 years to ensure it remains up to date and compliant with the law. It will be reviewed in May 2018 to update on introduction of the EU's General Data Protection Regulation (GDPR).

11. Declaration

I confirm I have read and understood SPPA's Data Protection Policy and will act in accordance with it.

I am connected with this organisation in my capacity as a

- ☐ Member of staff
- ☐ Volunteer
- ☐ Trustee/ management committee member

Signature:

Print name:

Date:

Please return this form to the Secretary.