**Data Guidance and Policy**

GDPR forms part of the data protection regime in the UK, together with the Data Protection Act 2018 (DPA 2018). It applies to personal data. This is information from which a living individual can be identified, either directly or indirectly (from other information held).

1.2 Personal data does not have to be written and includes visual, photographic, and other non-text data. This covers information held on computer, other electronic equipment, paper-based records, and other records (e.g. photographs).

2.1 Organisations or individuals holding personal data are data controllers. Many data controllers including SS must notify the Information Commissioner that we are processing personal data. The Information Commissioner maintains a public register of data controllers.

2.2 The Data Protection Commission has a list of standard purposes. In addition, SS is registered for “any other purpose that is deemed necessary and appropriate to enable the CIC to fulfill its objectives and be innovative and responsive”.

2.3 The Senior Information Risk Owner is responsible for ensuring there is a valid notification in the register of data controllers

3) HOLDING & TAKING CARE OF PERSONAL DATA

3.1 You are only allowed to use personal data for the purposes for which it was originally obtained. Personal information you hold must be:

• Processed lawfully, fairly, and in a transparent manner about individuals.

• Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall not be incompatible with the initial purposes.

• Must be adequate, relevant, and limited to what is necessary about the purposes for which they are processed.

Accurate and, where necessary kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regards to the purposes for which they are processed, is erased or rectified without delay.

• Kept in a format that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes subject to the implementation of the appropriate technical and organisation measures required by the GDPR to safeguard the rights and freedoms of individuals.

• Processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction, or damage, using appropriate technical or organisation measures.

3.3 Members of staff who, as part of their roles, are required to collect and maintain personal data must take good care of the data which they hold. There are two types of security breaches that SS must protect against (1) unauthorised access (2) data getting damaged, lost, or destroyed.

3.3.1 Unauthorised access:

• Personal information must be securely stored in a locked filing cabinet or protected by access permissions on SharePoint. Personal data must not be kept on a computer screen unless it is being processed and hard copies must not be left unattended. Such data must be kept in a closed file folder when on the desk. Staff, volunteers, and trustees should only have access to personal information when this is reasonable, relevant, and necessary to undertake their role within Silver Slippers.

• Trustees do not have the right of access to service user records, personnel files, or other personal information unless this information is relevant to a complaint, grievance, disciplinary or other formal investigation.

• Very occasionally it will be necessary to remove personal information/case files or other documents from Silver Slippers’ premises. This may be to allow records to be referred to during a meeting or conversation or to make such records available for scrutiny by a service user. Great care must be taken to ensure the security of such papers. Files removed from the office will be placed in an envelope marked ‘Private & Confidential’ with SS’s contact details on the outside and if it is necessary to leave files in a car they must be placed in the boot and not left on display. A note giving details of the file removed will be left at the office and recorded on the Log. Papers will be returned promptly.

• All personal and highly sensitive data sent via email should be protected by encryption with the use of appropriate subject line. Emails must be marked as ‘Private and Confidential’.

• Password protection/ Restricted Access will be used to restrict inappropriate access to personal and sensitive information.

• When disposing of confidential manual files all information must be shredded.

• Electronic files need to be deleted and removed from the recycle bin on SharePoint to prevent unauthorised access.

3.3.2 Damage, loss, or destruction: You must take reasonable steps to protect against the risks of damage, loss, or destruction of personal information

• SS have transitioned to cloud storage, it is the responsibility of each employee to follow advice from the IT contractors to save their work on the cloud (SharePoint) which works as a backup to protect against data loss.

• It is each employees’ responsibility to keep their machines compliant by performing regular system updates and following advice given by the IT contractors.

• Silver Slippers has software installed to protect against computer viruses.

• Measures must be taken to ensure Silver Slippers’ premises are protected from the risks of fire and theft as part of their risk assessment procedures.

4) OBTAINING AND USING PERSONAL DATA FAIRLY

 4.1 As a data controller SS must ensure that the rights of the data subjects under the legislation are preserved.

These rights are as follows:

• The right to be informed;

• The right of access;

• The right to rectification;

• The right to erasure;

• The right to restrict processing;

• The right to data portability;

• The right to object;

• Rights about automated decision-making and profiling.