STaSS Data Protection Policy MAY 2015

STaSS takes its responsibilities with regard to the management of the requirements of the Data Protection Act 1998 very seriously. The Act regulates the processing of information relating to living and identifiable individuals. This document provides the policy framework through which this effective management can be achieved.

1.0 Purpose and principles

The purpose of this policy is to ensure that STaSS, its Trustees and staff comply with the provisions of the Data Protection Act 1998 when processing personal data. Under the Act, data includes computerised records as well as manual filing and card indexes. Any infringement of the Act will be taken seriously by STaSS and may be considered under disciplinary procedures.

STaSS staff and Trustees are required to adhere to the eight principles of data protection as laid down by the Act. In accordance with those principles the data shall be:
1. Processed fairly
2. Obtained for specified and lawful purposes.
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept any longer than necessary
6. Processed in accordance with the “data subject’s” rights.
7. Securely kept
8. Not transferred to any other country without adequate protection

2.0 Responsibilities

2.1 Responsibilities of STaSS

STaSS recognises its responsibility under the Act and is the data controller.
The Director is the Data Protection Officer and is responsible for data protection compliance and is tasked with drawing up guidance and promoting compliance with this policy in such a way as to ensure the easy, appropriate and timely retrieval of information.

The Director will deal with notification matters, represent STaSS in any contact with the Information Commissioner, ensure that the STaSS Data Protection Policy is reviewed and updated at appropriate intervals, has access to all relevant documents relating to a legal compliance request, take the Act into consideration when setting up new systems or considering use of data for a new purpose and will make decisions [in consultation with the Trustees] regarding what information is released or exempted.
Individual members of staff will only be able to access information, which is relevant to their role.

All new members of staff should receive an introductory briefing on the Data Protection Act as part of STaSS’ induction procedures. Access to all computers and relevant software applications will be password protected, and staff and volunteers will only be able to access information, which is relevant to their role. Information held on laptops, netbooks etc. would be encrypted.

2.2 Staff Responsibilities

i] When staff members use personal information about service users, other staff members, volunteers or other individuals they must comply with the requirements of this policy.
ii] Staff members must ensure that:

- All personal information entrusted to them in the course of their employment is kept securely;
- Records are relevant i.e. only data that is needed is collected, accurate and up-to-date. Any errors must be corrected effectively and promptly;
- No personal information is disclosed either verbally or in writing, accidentally or otherwise to any unauthorised third party;
- Any infringement of the Act will be treated seriously by STaSS and may be considered under disciplinary proceedings;

- Photographs, recordings, videos or DVDs in which individuals are identifiable will only be used with an individual's written consent;
- Electronic equipment taken off site including laptops, memory sticks and mobile phones must not be left unattended or left in cars and if left at home must be put in a cupboard when not in use;
- Records are destroyed no later than 12 months after an individual e.g. a service user, volunteer or an unsuccessful job applicant has ceased to be in contact with STaSS;
- Text messages which enable an individual to be identified must be deleted at the earliest opportunity;
- Information no longer required is disposed of appropriately e.g. paper records should be shredded.

Staff who are unsure about who are authorised third parties to whom they can legitimately disclose personal data should seek advice from the Director.

3.0 Contractors, Temporary, Social work students and Voluntary Staff

- STaSS is responsible for the use of personal data by anyone working or volunteering on its behalf including contractors, social worker students, temporary staff or volunteers. Contractors, social work students, temporary staff and volunteers must ensure that:
- Any personal data collected or processed in the course of work/volunteering undertaken for STaSS, is kept securely and confidentially. This applies whether the data is an integral part of the work, or whether it is simply contained on media or in places which contractors/ volunteers/social work students/temporary staff need to access; it applies even if STaSS does not mention explicitly the requirement to adhere to the Data Protection Act.
- All personal data is returned to STaSS on completion of the work being undertaken, including any copies that have been made. Alternatively that the data is securely destroyed and that STaSS is informed by the contractor/ social work students/temporary member of staff or volunteer.
- STaSS must receive details of any disclosure of personal data to any other organisation or any person who is not a direct employee of the contractor.
- Any personal data made available by STaSS, or collected in the course of the work, is neither stored nor processed outside the UK unless written consent to do so has been received from STaSS.

All practical and reasonable steps are taken to ensure that contractors, social work students, temporary staff and volunteers do not have access to any personal data beyond what is essential for the work to be carried out properly.

4.0 Responsibilities of the Director and Service Manager

The Director must confirm to the Trustees annually that the requirements of this policy are being complied with.

The Service Manager will be the Data Protection Co-ordinator. The post holder will manage compliance with data protection legislation and STaSS' guidance in this area. The Director and the Service Manager will be knowledgeable and accessible points of contact within STaSS for people who have questions about data protection issues.

5.0 Subject Access Requests

STaSS is required to allow individuals to access their own personal data, which it holds via a Subject Access Request – Request for Personal Data. Any individual wishing to exercise this right should do so in writing to the Director and a charge may be made.

STaSS aims to comply with requests for access to personal information as quickly as possible but will ensure that it is provided within the 40-day limit set down by the Data Protection Act.

Individuals will not be entitled to access information to which any of the exemptions in the Act apply. However, only those specific pieces of information to which the exemption applies will be withheld, and information covered by an exemption will be subject to review by the Director.

6.0 Personal Data Systems

The Director must ensure that a register of all systems [both paper and electronic] which include personal data and sensitive personal data is held by STaSS.

7.0 Charges

STaSS will charge £50 to make a subject access request, however, it reserves the right to review the fee at any time.

8.0 Data Security Breach

Any breach of the Data Protection Act and the requirements of this policy should be reported to the Director as soon as possible. A report of a suspected breach of the Act will be dealt with in accordance with STaSS' "Procedures for the Management of a Suspected Data Security Breach".

9.0 Complaints

STaSS' "Complaints Policy" will be followed. However, if an individual remains dissatisfied with the outcome of a complaint, they may seek an independent review from the Information Commissioner.
Requests for review should be made in writing to:
The Information Commissioner, Wycliffe House, Water Lane, Wilmslow Cheshire, SK9 5AF, Tel: 01625 545 700, Fax: 01625 545 510

This policy was explained to me and I have also read and understood its content. I promise to abide by it now and after my engagement with STaSS.

Signed _____

Print Name _____

Date _____

Policy Review

The Director and Board of Trustees are responsible for reviewing this policy annually and ensuring that it is compliant with current legislation and good practice.

REVIEWED MAY 2015, NEXT SCHEDULED REVIEW MAY 2016