Association for Solution Focused Hypnotherapists

DATA PROTECTION POLICY

INTRODUCTION

This document is the data protection policy and procedure for the Association of Solution Focused Hypnotherapists.

The Data Protection Act 1998 (DPA) governs the processing of personal data including the release of personal data, in the UK. It requires that personal data and sensitive personal data must be processed by data controllers in accordance with the eight data protection principles. The DPA implements the EU Data Protection Directive 95/46/EC.

The AfSFH is a data controller under the DPA.

All processing of personal data by or on behalf of the AfSFH must comply with the DPA.

AIMS OF THE POLICY

- To state the AfSFH commitment to compliance with the DPA and the eight data protection principles
- To outline how the AfSFH will achieve compliance with the DPA
- To state the responsibility of all those working for or on behalf of the AfSFH to comply with the DPA.

SCOPE

This policy applies to all personal information as defined by the DPA, in both electronic and paper form, held by the AfSFH, transferred to, or exchanged with third parties, or held by third parties on behalf of the AfSFH.

This policy is related to the Information security policy and the ICT user policy, and informs other policies such as HR policies and data sharing policies.

ROLES AND RESPONSIBILITIES

The ultimate responsibility for the AfSFH compliance with the DPA lies with the Executive Committee and Registrar who is the Data Protection Coordinator for the AfSFH.

Day to day responsibilities for data protection matters may be delegated to the other roles within AfSFH.

Therapists within every business area are responsible for implementing data protection policies and procedures in their areas including with the third parties that they liaise with.

All those working for and on behalf of the AfSFH must comply with this policy. The Trustees are responsible for maintaining this policy and may delegate responsibility for approving changes to the policy to the Executive Committee.

POLICY REVIEW

This policy will be reviewed annually, or more frequently in the event of any legislative or regulatory changes.

COMMUNICATION

Awareness of this policy will be included on the website for all new members working for and on behalf of the AfSFH.

In addition, all members should obtain regular data protection training as part of a CPD program.

Copies of this and other policies and guidelines are available on the AfSFH website

COMPLIANCE

All those working for or on behalf of the AfSFH are required to comply with this policy.

Any alleged breach of this policy may result in an investigation which may result in action being taken by the AfSFH up to and including removal from the Associations membership.

The AfSFH will cooperate with law enforcement authorities if a criminal violation is suspected, and it reserves the right to claim compensation from the individual(s) through normal lawful processes in the event that the AfSFH suffers damage.

Section 55 (1) of the Data Protection Act 1998 states that:

“It is an offence for a person, knowingly or recklessly, without the consent of the data controller to:

- obtain or disclose personal data or the information contained in personal data,

or

- procure the disclosure to another person of the information contained in personal data.”

Definitions of personal data and sensitive personal data used within the Data Protection Act 1998 are:

- **Personal data**

Personal data is information which relates to a living individual who can be identified from that data or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

- **Sensitive personal data**

Sensitive personal data is personal data which consists of data related to the data subject's racial or ethic origin political opinions, religious or similar beliefs, trade union membership, physical or mental health, sexual life, the commission of offences or criminal proceedings.

POLICY STATEMENTS

The data protection principles state that all those working for and on behalf of the AfSFH must comply with the data protection principles enshrined in the act which state that personal data must be:

- Processed fairly and lawfully
- Only obtained for specified and lawful purposes and not processed in a manner incompatible with those purposes
- Adequate, relevant and not excessive in relation to the purposes for which it is held.
- Accurate and, where necessary, kept up to date
- Kept for only as long as is necessary
- Processed in accordance with the rights of data subjects under the act, including the data subjects' right of access and right to object to the processing of their data in certain circumstances
- Protected from unauthorised and unlawful processing; accidental loss, destruction or damage by having appropriate technical and organisational measures in place
- Only transferred outside the European Economic Area (EEA) where an adequate level of protection for the data can be ensured.

PROCESSING AND USE OF PERSONAL DATA

The AfSFH processes personal data about members, those working for and on behalf of the AfSFH, stakeholders, and other individuals, in order to fulfil its purpose and meet its legal obligations.

Personal data will only be processed lawfully and fairly in order to fulfil AfSFH purpose and meet its legal obligations.

All those working for an on behalf of the AfSFH must follow AfSFH procedures relating to the processing and use of personal information.

The AfSFH will inform data subjects of the uses of their data in accordance with the requirements of the DPA.

USE OF MONITORING AND SURVEILLANCE TECHNOLOGY

Any deployment of audio recording, video recording, CCTV or other monitoring and surveillance technologies will be in compliance with the DPA.

RIGHT TO ACCESS INFORMATION AND SUBJECT ACCESS REQUESTS

Anyone has the right to access personal data that is being held about them by the AfSFH.

Anyone wishing to exercise this right should make the request in writing to the Records Manager, CPHT, 8 – 10 Whiteladies Road, Clifton, Bristol BS8 1PD

Requests for personal information will be handled in accordance with the Data Protection Act 1998.

COMPLAINTS PROCEDURE

Anyone who considers that this policy has not been followed may make a complaint following AfSFH complaints procedure.

DATA SECURITY

All users of personal information held by the AfSFH must comply with the ICT User policy and are responsible for ensuring that any personal information that they process is kept securely and is not disclosed in any form to any unauthorised third party.

Where personal information is protectively marked, the processing of that information must be in accordance with any AfSFH policy and procedures for the processing of protectively marked information.

AfSFH will seek to ensure that all data that has been authorised to be sent off site is encrypted.

DATA SHARING

Any sharing of personal data with external third parties must comply with any AfSFH data sharing policy and procedures.

INCIDENT REPORTING

All those working for and on behalf of the AfSFH must report any information security incident which involves the loss or potential loss or the unauthorised disclosure of personal information by following the appropriate incident reporting procedures.

GLOSSARY

Data	Information about an individual which: • is being processed by means of equipment operating automatically in response to instructions given for that purpose • is recorded with the intention that it should be processed by means of such equipment • is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system.
Data controller	• A person who either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data are, or are to be, processed. The term comprises not only individuals but also organisations such as companies and other corporate bodies of persons
Data processor	• Any person, other than an employee of the data controller, who processes the data on behalf of the data controller
Data protection coordinator	• The senior person in an organisation who has responsibility for data protection
Data subject	• Any living individual who is the subject of personal data
Processing	• Any operation or set of operations performed upon personal data, whether or not by automatic means. These include collecting, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
Relevant filing system	• Any set of manual information relating to individuals, which is structured, either by reference to individuals or by reference to criteria relating to individuals, (that is their name or identifying code number) in such a way that specific information relating to a particular individual is readily accessible