Data Protection Policy

Sen Talk is committed to a policy of protecting the rights and privacy of individuals, including service users, staff, volunteers, colleagues and affiliates of the organisation, in accordance with the General Data Protection Regulations (GDPR) May 2018.

The new regulatory environment demands higher transparency and accountability in how organisations manage and use personal data. It also accords new and stronger rights for individuals to understand and control that use.

The GDPR contains provisions that Sen Talk will need to be aware of as both data controllers and data processers, including provisions intended to enhance the protection of individuals personal data. For example, the GDPR requires that: We must ensure that our privacy notices are written in a clear, plain way that is also translatable for all to understand. This may require translation to different languages, braille or other communication types where appropriate.

The organisation controls and processes the follow data:

- Information about service users, volunteers and staff
- The recruitment and payment of staff and volunteers
- The administration of courses and programmes
- Recording service users progress, attendance and conduct
- Collecting fees of any kind
- Images and information for marketing purposes

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) Sen Talk must ensure that all this information about individuals is collected and used fairly, stored safely and securely, and not disclosed to any third party unlawfully without explicit consent or lawful obligation.

Compliance

This policy applies to all service users, staff, volunteers, colleagues and affiliates of the organisation. Any breach of this policy or of the Regulation itself will be considered an offence and will invoke the organisations disciplinary procedure. As a matter of best practice, other agencies and individuals working with Sen Talk and who have access to personal information, will be expected to read and comply with this policy. Additionally,

staff members and volunteers are required to read and comply with the confidentiality policy and sign the confidentiality agreement within their individual contract with Sen Talk.

This policy will be reviewed annually and amended as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments to the GDPR and other relevant legislation. The Code of Practice on GDPR for Sen Talk gives further detailed guidance and Sen Talk undertakes to adopt and comply with this Code of Practice.

General Data Protection Regulation (GDPR)

This piece of legislation comes in to force on the *25th May 2018*. The GDPR regulates the controlling and processing of personal data and protects the rights and privacy of all living individuals (including children), for example by giving all individuals who are the subject of personal data a general right of access to the personal data which relates to them. Individuals can exercise the right to gain access to their information by means of a 'subject access request'. Personal data is information relating to an individual and may be in hard or soft copy (paper/manual files; electronic records; photographs; CCTV images) and may include facts or opinions about a person.

Data control

Sen Talk will be the 'data controller' under the terms of the legislation – this means it is ultimately responsible for controlling the use and processing of the personal data. The organisation appoints a Data Protection Officer (DPO), currently the Director who is available to address any concerns regarding the data held by organisation and how it is processed, held and used. Sen Talks Board of Trustees will oversee this policy. The Director is responsible for all day-to-day data protection matters and will be responsible for ensuring that all members of staff and relevant individuals abide by this policy, and for developing and encouraging good information handling within the organisation.

Responsibility

Compliance with the legislation is the personal responsibility of all members of Sen Talk who process personal information. Individuals who provide personal data to the organisation are responsible for ensuring that the information is accurate and up to date.

Data Protection principles

The legislation places a responsibility on every data controller to process any personal data in accordance with the eight principles.

More detailed guidance on how to comply with these principles can be found following this link to the ICO's website (www.ico.gov.uk) In order to comply with its obligations, Sen Talk undertakes to adhere to the eight principles:

1. Process personal data fairly and lawfully

Sen Talk will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the identity of the data controller, the purposes of the processing, any disclosures to third parties that are envisaged; given an indication of the period for which the data will be kept, and any other information which may be relevant.

2. Purpose limitation

Sen Talk will process data for the specific and lawful purpose for which it is collected and not further process the data in a manner incompatible with this purpose. The organisation will ensure that data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. Data minimisation

Sen Talk will ensure all data that is collected is adequate, relevant and limited to what is necessary in relation to the purposes. The organisation will not seek to collect any personal data which is not strictly necessary for the purpose for which it was obtained. Forms for collecting data will always be drafted with this mind. If any irrelevant data are given by individuals, they will be destroyed immediately.

4. Keep personal data accurate and, where necessary, up to date

Sen Talk will review and update all data on a regular basis. It is the responsibility of the individuals giving their personal data to ensure that this is accurate, and each individual should notify the organisation if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the organisation to ensure that any notification regarding the change is noted and acted on.

5. Storage limitation

Sen Talk will not retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements. This means Sen Talk will undertake a regular review of stored data and will dispose of unnecessary data in a manner

that protects the rights and privacy of the individual involved. For example: secure electronic deletion, shredding and disposal of hard copy files as confidential waste.

6. Process personal data in accordance with the rights of the data subject under the legislation

Individuals have various rights under the legislation including a right to:

- be told the nature of the information the organisation holds and any parties to whom this may be disclosed
- prevent processing likely to cause damage or distress
- prevent processing for purposes of direct marketing
- be informed about the mechanics of any automated decision-making process that will significantly affect them
- not have significant decisions that will affect them taken solely by automated process
- sue for compensation if they suffer damage by any contravention of the legislation
- take action to rectify, block, erase or destroy inaccurate data
- request that the Office of the Information Commissioner assess whether any provision of the Act has been contravened

7. Integrity and confidentiality

Sen Talk will ensure data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. All members of staff are responsible for ensuring that any personal data which they hold is kept securely and not disclosed to any unauthorised third parties. Sen Talk will ensure that all personal data is accessible only to those who have a valid reason for using it. The organisation will have in place appropriate security measures e.g. ensuring that hard copy personal data is kept in lockable filing cabinets/cupboards with controlled access (with the keys then held securely in a key cabinet with controlled access):

- keeping all personal data in a lockable cabinet with key-controlled access
- password protecting personal data held electronically
- archiving personal data which are then kept securely (lockable cabinet)
- Placing any PCs or terminals that show personal data so that they are not visible except to authorised staff
- ensuring that PC screens are not left unattended without a password protected screen-saver being used

In addition, Sen Talk will put in place appropriate measures for the deletion of personal data. Manual records will be shredded or disposed of as 'confidential waste' and appropriate contract terms will be put in place with any third parties undertaking this work.

Hard drives of redundant PCs will be wiped clean before disposal or if that is not possible, destroyed physically. A log will be kept of the records destroyed.

This policy also applies to staff and service users who process personal data 'off-site', e.g. when working at home.

8. **Ensure that no personal data is transferred to a country or a territory outside the European Economic Area (EEA) unless that country or territory ensures adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

Sen Talk will not transfer data to such territories without the explicit consent of the individual. This also applies to publishing information on the Internet - because transfer of data can include placing data on a website that can be accessed from outside the EEA - so the organisation will always seek the consent of individuals before placing any personal data (including photographs) on its website. If the organisation collects personal data in any form via its website, it will provide a clear and detailed privacy statement prominently on the website, and wherever else personal data is collected.

Consent

Obtaining consent

Although it is not always necessary to gain consent from individuals before processing their data, it is often the best way to ensure that data is collected and processed in an open and transparent manner. Consent is especially important when Sen Talk is processing any sensitive data, as defined by the legislation. The organisation understands consent to mean that the individual has been fully informed of the intended processing and has signified their agreement whilst being of a sound mind and without having any undue influence exerted upon them. Consent obtained on the basis of misleading information will not be a valid basis for processing. Consent cannot be inferred from the non-response to a communication.

Managing consent

The organisation will update obtain separate photo consent forms on each occasion that a photograph is taken, with explicit instruction of the intended use of the data. Consent will renewed every 12 months, to ensure that service users consent is accurate and recent.