Data Protection Policy & GDPR Statement

1 In relation to all Personal Data the Association shall at all times comply with all applicable legislation including the Data Protection Act 1998 as a data controller. If necessary including maintaining a valid and up to date registration or notification under the Data Protection Act 1998 covering the data processing to be performed in connection with our services.

2 The Association shall only undertake processing of Personal Data reasonably required in connection with the Services and shall not transfer any Personal Data to any Country or territory outside the geographical area of the European Union.

3 The Association shall not disclose Personal Data to any third parties other than to the extend required under a court order or by virtue of a legal requirement provided that disclosure under clause 1 is made subject to written terms substantially the same as, and no less stringent than, the clauses 1-8 and that the Association shall give notice in writing to the Service User and the Council of any disclosure of Personal Data it is required to make under Clause 1 immediately it becomes aware of such a requirement. Copying of case files for Councils/Courts will incur an admin and printing levy.

4 The Association shall bring into effect and maintain all technical and organisational measures to prevent unauthorised or unlawful processing of Personal Data and accidental loss or destruction of or damage to Personal Data including but not limited to taking reasonable steps to ensure the reliability of staff having access to the personal data.

5 The Association may, at reasonable levels be asked or instructed by Courts or Councils request a written description of the technical and organisational method employed by the Association in order to comply with its obligations under clause 4. Within 30 days of such a request by Courts or Councils to provide and supply written particulars if all such measures detailed to a reasonable level such that the Council can determine whether or not it is compliant with the Data Protection Act 1998.

6 Current Client records up to 3 years kept in secure filing cabinets/database. Records 3-5 years: Paper form registration and short form records securely archived, after 5 years records are destroyed by secured means. Client Information on database kept for 6 years after date of death and then destroyed. Short form Historical Records 1880's-1990's held securely at The Keep, East Sussex Records Office, Woollards Way, Brighton BN1 9BP.

Employee Records for current staff are kept in secure filing cabinets. Ex-employee records shredded after 12 months of leave date.

7 Subject Access Request (SAR) Clients wishing to view their files may have access in the presence of Association staff personnel. Viewing, discussion, releasing and copying of records to third parties other than in the case of Clause 3 are prohibited. Consent to Share Information Form must be completed prior to any information being printed or released. Again time spent collating information and printing will incur charges as per our Service User Support Charges. Some information such as support workers names may be deleted to protect their identity. Signatures will be required to ensure safe keeping of sensitive information protecting both the client and support workers.

8 Personal details of individuals, on paper, must be kept in a secure place with keys only accessible to SDA manager and workers. Laptops must not hold direct access to personal data or contact information unless accessed via SDAD password protected server. Details of client case file or information from the database may not be emailed or sent electronically to anyone unless agreed with SDA's Manager.

9 All work staff carried out on a laptop/computers must be stored and saved directly to the SDAD Server and not on Laptop C Drives or USB sticks.

GDPR Compliance Statement

Introduction

The EU General Data Protection Regulation ("GDPR") comes into force across the European Union on 25th May 2018 and brings with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, the GDPR has been designed to meet the requirements of the digital age.

The 21st Century brings with it broader use of technology, new definitions of what constitutes personal data, and a vast increase in cross-border processing. The new Regulation aims to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

Our Commitment

The Sussex Deaf Association are committed to ensuring the security and protection of the personal information that we process, and to provide a compliant and consistent approach to data protection. We have always had a robust and effective data protection program in place which complies with existing law and abides by the data protection principles. However, we recognise our obligations in updating and expanding this program to meet the demands of the GDPR and the UK's Data Protection.

The Sussex Deaf Association are dedicated to safeguarding the personal information under our remit and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for the new Regulation. Our preparation and objectives for GDPR compliance have been summarised in this statement and include the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum and ongoing compliance.

How we are Preparing for the GDPR

The Sussex Deaf Association already have a consistent level of data protection and security across our organisation, however it is our aim to be fully compliant with the GDPR by 25th May 2018.

Our preparation includes: -

- Information Audit - carrying out a company-wide information audit to identify and assess what personal information we hold, where it comes from, how and why it is processed and if and to whom it is disclosed.

- Policies & Procedures - revising/implementing new data protection policies and procedures to meet the requirements and standards of the GDPR and any relevant data protection laws, including: -

- Data Protection – our main policy and procedure document for data protection has been overhauled to meet the standards and requirements of the GDPR.

Accountability and governance measures are in place to ensure that we understand and adequately disseminate and evidence our obligations and responsibilities; with a dedicated focus on privacy by design and the rights of individuals.

- Data Retention & Erasure – we have updated our retention policy and schedule to ensure that we meet the 'data minimisation' and 'storage limitation' principles and that personal information is stored, archived and destroyed compliantly and ethically. We have dedicated erasure procedures in place to meet the new 'Right to Erasure' obligation and are aware of when this and other data subject's rights apply; along with any exemptions, response timeframes and notification responsibilities.

- Data Breaches – our breach procedures ensure that we have safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. Our procedures are robust and have been disseminated to all employees, making them aware of the reporting lines and steps to follow.

- International Data Transfers & Third-Party Disclosures – where Sussex Deaf Association stores or transfers personal information outside the EU, we have robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of the data. Our procedures include a continual review of the countries with sufficient adequacy decisions, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without. We carry out strict due diligence checks with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

- Subject Access Request (SAR) – we have revised our SAR procedures to accommodate the revised 30-day timeframe for providing the requested information and for making this provision free of charge. Our new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- Legal Basis for Processing - we are reviewing all processing activities to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, we also maintain records of our processing activities, ensuring that our obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Bill are met.

- Privacy Policy – we have revised our Privacy Policy to comply with the GDPR, ensuring that all individuals whose personal information we process have been informed of why we need it, how it is used, what their rights are, who the information is disclosed to and what safeguarding measures are in place to protect their information.

- Obtaining Consent - we have revised our consent mechanisms for obtaining personal data, ensuring that individuals understand what they are providing, why and how we use it and giving clear, defined ways to consent to us processing their information. We have developed stringent processes for recording consent, making sure that we can evidence an affirmative opt-in, along with time and date records; and an easy to see and access way to withdraw consent at any time.

- Data Protection Impact Assessments (DPIA) – where we process personal information that is considered high risk, involves large scale processing or includes special category/criminal conviction data; we have developed stringent procedures and assessment templates for carrying out impact assessments that comply fully with the GDPR's Article 35 requirements. We have implemented documentation processes that record each assessment, allow us to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- Processor Agreements – where we use any third-party to process personal information on our behalf (i.e. Payroll, Recruitment, Hosting etc), we have drafted compliant Processor Agreements and due diligence procedures for ensuring that they (as well as we), meet and understand their/our GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and compliance with the GDPR.

- Special Categories Data - where we obtain and process any special category information, we do so in complete compliance with the Article 9 requirements and have high-level encryptions and protections on all such data. Special category data is only processed where necessary and is only processed where we have first identified the appropriate Article 9(2) basis or the Data Protection Bill Schedule 1 condition.
Where we rely on consent for processing, this is explicit and is verified by a signature, with the right to modify or remove consent being clearly signposted.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals both employee and service user can enforce their data protection rights, we provide easy to access information via our website, in the office, during induction etc of an individual's right to access any personal information that Sussex Deaf Association processes about them and to request information about: -

- What personal data we hold about them
- The purposes of the processing
- The categories of personal data concerned
- The recipients to whom the personal data has/will be disclosed
- How long we intend to store your personal data for
- If we did not collect the data directly from them, information about the source
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this
- The right to request erasure of personal data (where applicable) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing from us and to be informed about any automated decision-making that we use
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances

Information Security & Technical and Organisational Measures

The Sussex Deaf Association takes the privacy and security of individuals and their personal information very seriously and take every reasonable measure and precaution to protect and secure the personal data that we process. We have robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction and have several layers of security measures, including: -

Access Controls, Passwords, IT & Authentication

GDPR Roles and Employees

The Sussex Deaf Association have designated The Manager as our Appointed Person. The Manager is responsible for promoting awareness of the GDPR across the organisation, assessing our GDPR readiness, identifying any gap areas and implementing the new policies, procedures and measures.

The Sussex Deaf Association understands that continuous employee awareness and understanding is vital to the continued compliance of the GDPR and have involved our employees in our preparation plans. Training will be implemented nearer the time or as part of induction/annual training programmes.

Date adopted: 22 November 2007

Next Review May 2019

MC Signature 24/8/18