Hertfordshire Hearing Advisory Service	**HERTFORDSHIRE HEARING ADVISORY SERVICE POLICIES AND PROCEDURES**
	P19 – GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

Rationale

Hertfordshire, Suffolk, Bedfordshire, Hearing Advisory Service (HAS) is committed to a policy of protecting the rights and privacy of individuals, including clients, staff and others, in accordance with the General Data Protection Regulation (GDPR) May 2018.

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

The GDPR contains provisions that HAS will need to be aware of as data controllers, including provisions intended to enhance the protection of personal data. For example, the GDPR requires that:

We must ensure that our charities privacy notices are written in a clear, plain way that staff, volunteers and clients will understand.

HAS needs to process certain information about its individuals

1. The recruitment and payment of staff.
2. Staff files, Volunteer files, client's records.
3. The administration of schedules and collection of client data.
4. The administration of News and Views.
5. Complying with legal obligations to funding bodies and government including local government.

To comply with various legal obligations, including the obligations imposed on it by the General Data Protection Regulation (GDPR) HAS 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.

Compliance

This policy applies to all staff, volunteers and clients of HAS. Any breach of this policy or of the Regulation itself will be considered an offence and the Charity's disciplinary procedures will be invoked.

As a matter of best practice, other agencies and individuals working with HAS and who have access to personal information, will be expected to read and comply with this policy.

This policy will be updated 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 DPR for HAS gives further detailed guidance and HAS undertakes to adopt and comply with this Code of Practice.

P19 – GENERAL DATA PROTECTION REGULATION (GDPR) POLICY

General Data Protection Regulation (GDPR)
This legislation comes in to force on the 25th May 2018. The GDPR regulates the 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), and may include facts or opinions about a person.

Responsibilities under the GDPR
HAS 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 charity appoints a Data Protection Officer (DPO), currently the CEO who is available to address any concerns regarding the data held by the charity and how it is processed, held and used.

HAS also has a nominated board of trustees who oversees this policy. The CEO 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 HAS.

Data Protection Principles
The legislation places a responsibility on data controller to process any personal data in accordance with the eight principles. To comply with its obligations, CEO undertakes to adhere to the eight principles:

1. Process personal data fairly and lawfully. HAS will make all reasonable efforts to ensure that individuals who are the focus of the personal data (data subjects) are informed of the purposes of the processing, any disclosures to third parties that are envisaged'
2. Process the data for the specific and lawful purpose for which it collected that data and not further process the data in a manner incompatible with this purpose. HAS will ensure that the reason for which it collected the data originally is the only reason for which it processes those data.
3. Ensure that the data is adequate, relevant and not excessive in relation to the purpose for which it is processed. HAS 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.
4. Keep personal data accurate and, where necessary, up to date. HAS 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 everyone should notify the Charity if, for example, a change in circumstances mean that the data needs to be updated. It is the responsibility of the Charity to ensure that any notification regarding the change is noted and acted on.

5. Only keep personal data for as long as is necessary. HAS undertakes not to retain personal data for longer than is necessary to ensure compliance with the legislation, and any other statutory requirements.

   HAS will undertake a regular review of the information held and implement a weeding process. HAS will dispose of any personal data in a way that protects the rights and privacy of the individual concerned (e.g. secure electronic deletion, shredding and disposal of hard copy files as confidential waste). A log will be kept of the records destroyed.

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 HAS holds and any parties to whom this may be disclosed.
   - prevent processing for purposes of direct marketing.
   - act 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. HAS will only process personal data in accordance with individuals' rights.

7. Put appropriate technical and organisational measures in place against unauthorised or unlawful processing of personal data, and against accidental loss or destruction of data.

   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. HAS will ensure that all personal data is accessible only to those who have a valid reason for using it. HAS 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, CCTV camera screens etc. that show personal data so that they are not visible except to authorised staff.

   In addition, HAS 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 volunteers who process personal data 'off-site', e.g.

when working at home, and in circumstances additional care must be taken regarding the security of the data.

7. 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. HAS 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 - HAS will always seek the consent of individuals before placing any personal data (including photographs) on its website.
   If the Charity 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 as a basis for processing

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 HAS is processing any sensitive data, as defined by the legislation. HAS understands consent to mean that the individual has been fully informed of the intended processing.

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. “Personal Details”

- For the purposes of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 you consent to the Charity holding and processing personal data including sensitive personal data of which you are the subject, details of which are specified in the Charity’s data protection policy.
- This will include marketing images and the College. HAS will ensure that any forms used to gather data on an individual will contain a statement explaining the use of that data, how the data may be disclosed and indicate whether or not the individual needs to consent to the processing.

HAS will ensure that if the individual does not give his/her consent for the processing, and there is no other lawful basis on which to process the data, then steps will be taken to ensure that processing of that data does not take place.

Subject Access Rights (SARs)

Individuals have a right to access any personal data relating to them which are held by the Charity. Any individual wishing to exercise this right should apply in writing to the CEO. Any member of staff receiving a SAR should forward this to the CEO.

1.1 We will not usually charge a fee for responding to a data subject access request. We may, however, charge a reasonable fee (based on the administrative cost of providing the information) for responding to a request:

1.1.1 that is manifestly unfounded or excessive, eg repetitive; or

1.1.2 for further copies of the same information.

Under the terms of the legislation, any such requests must be complied with within 40 days. For detailed guidance on responding to SARs'.

Disclosure of Data

Only disclosures which have been notified under the Charity's DP notification must be made and therefore staff and volunteers should exercise caution when asked to disclose personal data held on another individual or third party.

HAS undertakes not to disclose personal data to unauthorised third parties, including family members, friends, government bodies and in some circumstances, the police. Legitimate disclosures may occur in the following instances:

- the individual has given their consent to the disclosure.
- the disclosure is required for the performance of a contract. There are other instances when the legislation permits disclosure without the consent of the individual.

Publication of Charity's Information

HAS publishes various items which will include some personal data, e.g.

- internal telephone directory.
- event information.
- news and views
- photos and information in marketing materials.

It may be that in some circumstances an individual wishes their data processed for such reasons to be kept confidential, or restricted Charity's access only. It is HAS policy to offer an opportunity to opt-out of the publication of such when collecting the information.

Email

It is the policy of HAS ensures that senders and recipients of email are made aware that under the DPA, and Freedom of Information Legislation, the contents of email may have to be disclosed in response to a request for information. One means by which this will be communicated will be by a disclaimer on the Charity's email. Under the Regulation of Investigatory Powers Act 2000, Lawful Business Practice

Regulations, any email sent to or from the Charity may be accessed by someone other than the recipient for system management and security purposes.

Procedure for review

This policy will be updated as necessary to reflect best practice or future amendments made to the General Data Protection Regulation (GDPR) May 2018 and Data Protection Act 1998. Please follow this link to the ICO's website (www.ico.gov.uk) which provides further detailed guidance on a range of topics including individuals' rights, exemptions from the Act, dealing with subject access requests, how to handle requests from third parties for personal data to be disclosed etc. You may find it helpful to read the Guide to Data Protection which is available from the website. For help or advice on any data protection or freedom of information issues, please do not hesitate to contact:

The Data Protection Officer (DPO): Philip Linnegar CEO