



GDPR Policy

The Information Commissioner's Office (ICO), tell us that General Data Protection Regulation (GDPR) policies must be written in plain and simple language without any jargon or 'legal speak'.

Aim

The aim of this policy is to ensure we at Steven Hale Hearing comply with the General Data Protection Regulations (GDPRs) which apply to everyone who holds personal data, from 25th May 2018.

Overview

General Data Protection Regulations (GDPRs) have been made to give individuals more control about what happens to the personal data they provide to us. From 25th May 2018 onwards, your personal data cannot be gathered, stored or processed unless one of the six legal basis apply. Also, it must be destroyed if its purpose has ended. If you request details of any personal data held about you, the company must send it to you without charging you a fee or any other cost. This way, you will know that we have your personal data because you have allowed us to have it, or that we are storing and processing it because of one of the six legal basis.

However, personal data that we have in our records from before the 25th May 2018, will still be valid, but will now become subject to our storage, processing and destruction policy. All non-relevant data will be destroyed. This means that we will look at all the information we hold, and either be able to give a valid reason to keep it or destroy it.

Policy

To comply with GDPR and protect personal data, we will:

1. Make an initial review of the data we already have to sort out which is 'personal data' and which is 'non-personal data', whether it is held on paper or computer systems. GDPR only applies to personal data.
2. If a person cannot be identified from the data, then it will be called non-personal data, and the rules will not apply to it.
3. All personal data will be assessed to establish if it is also 'sensitive' data. Sensitive data is information which may reveal something about you that you may not want everyone to know, such as your sexuality, beliefs, any

medical issues or disabilities, political views and issues from your past. Any sensitive personal data will be treated with greater security by means of...see 9 below.

4. Hand written personal data will be stored in a locked office with named and limited people allowed to access it.
5. Hand written sensitive personal data will be stored in a locked drawer or cabinet within a locked office with only Steven Hale able to access it.
6. All handwritten personal data will be transferred to an electronic medium and then shredded as soon as practicable. No handwritten personal data will be left unattended on any staff member's desk.
7. We will obey a 'clear desk' order, not leave any personal data unattended on any desk, and shred handwritten personal data as soon as possible.
8. Electronic personal data will be stored on computers which are password protected. The computers automatically lock after a short period of not being used.
9. Electronic personal data which is sensitive will be stored on computers which are password protected. The computers automatically lock after a short period of not being used.
10. There may be certain situations, such as repair of hearing aids, where we need to share your personal information with hearing aid manufacturers to fulfil our obligations to you.
11. If our computers are lost or stolen, they remain password protected. Good practice suggests we would inform the ICO within 72 hours as this may be considered a 'breach'.
12. All electronic personal data will be deleted from files once it is no longer needed. An annual review will take place to ensure this has happened, and a record will be made that this has occurred.
13. From 25th May 2018, all new employees, suppliers, customers and other agencies will be asked for their consent for us to harvest, store, process and destroy personal information. We at Steven Hale Hearing understand that consent will **not** be legal if it is gained via a pre-ticked box, or with only an 'OPT OUT' option. Under GDPR you must do something physical which means you have given your consent. This will include you putting a tick in a box, signing to say that you consent/opt in, or even telling someone that you consent/opt in.
14. This will not apply to personal information prior to 25th May 2018 so long as we can justify our reasons for harvesting, storing and processing it. If not, we will destroy it, and a record will be made.
15. Whether your personal data is held on paper or computer, you will be able to see it free of charge and request that we destroy it if required or say that we can keep using it as we are. A record will be made of these actions.
16. You will still be able to 'unsubscribe' from our site or digital marketing platforms. If we then contact you after you have unsubscribed, we will be breaching the GDPR.
17. Any information required by Human Resources (HR) will be kept for a period of seven years. This is a legal requirement so that if you have any

- claims against us in that time we will still have your records. After this period your records will be destroyed and a record made.
18. We must tell everyone involved with us that we are complying with GDPR, so our website and emails will be updated to reflect this.
 19. Our website will tell all visitors that we are GDPR compliant and invite them to read more about our policy by clicking on a link.
 20. We will add a line to our business email signature to show that we are GDPR compliant and advise who you can contact if you wish to discuss our GDPR policy.
 21. A poster will be displayed in our office to raise and maintain awareness of GDPR, and to inform all visitors of our policy.
 22. If you have any questions, please speak to Director Steven Hale as he is the person responsible for complying with GDPR.
 23. Prior to 25th May 2018 we will only process your personal data if we can justify that it is in your best interests. If one of the six legal basis for doing this is not met, then we will destroy your data and a record will be made.
 24. If we discover a data breach, we will report it to the ICO within 72 hours.
 25. Every year we will review the personal data that we hold. We will record that this has taken place.

If you have any questions about this information, please speak to Director Steven Hale who will be happy to help you.

Privacy and Data Protection is everyone's responsibility, and we are proud to uphold GDPR to ensure that all personal and sensitive data held by Steven Hale Hearing is treated correctly.

For any further information, please look at the Information Commissioners Office (ICO) on www.ico.org.uk



