Sarah Maidment Massage Therapist Privacy Policy

This privacy policy is for Sarah Maidment Massage Therapist, 90 Chediston Street, Halesworth IP198BJ. Telephone 07484243208. Email info@sarahmaidment.co.uk

Policy Purpose

This policy outlines my privacy and data protection policy, and thus how I comply with the GDPR.

GDPR Registration

I am registered with the ICO as part of my GDPR compliance.

Policy Content

1.The data that I process and how it flows into, through and out of my business.

Data comes into my business in 8 ways:

a. Via email messages to me from potential clients (PC) and clients(C) that have my email
b. Via text messages (as above)
c. Via my website
d. Via posts/reviews on my facebook business page and other digital platforms e.g. my website
e. Via Facebook Messenger to my business page
f. Via Facebook Messenger to my personal page
g. Via phone calls and the written notes I take for these
h. Via face to face consultation
i. Via event sign in sheets
j. Via Instagram, GoogleMyBusiness, Yelp and other online business tools which may be added in the future.

It flows through my business via:

- My laptop - which is used at home and away from the home for work and study purposes
- My smart phone - everywhere I go
- My paper file - occasionally from home to a client's house and back if I am treating outside the home or at an event e.g. providing pre and post event massage.

Data flows out of my business as follows:

Appointment reminders:

- A third party system may be used to provide appointment confirmations as follows:
    - Booking confirmation
    - Appointment reminders
    - Post appointment follow up
- In the above scenarios the following client information will be input to the system purely for the above purposes:
    - Customer email address, name, date of birth, address
    - Customer appointment date/time, referral source, marketing/contact preferences where these are known/supported by the system

Marketing and general communications

- A third party system may be used for emailing customers with latest offers, new services or other relevant business information (subject to relevant consents being in place).
- In the above scenario the following client information will be put into the system purely for the above purposes:
    - Customer email address and name, marketing consent
- Where a client has left an open review on my business e.g. on Facebook this may be shared by me to my website either via an automated feed or manually. If a client does not leave a review but sends me feedback privately this feedback may be posted to social media or my website but would be anonymised so as the client is not identifiable.

In rare instances, data may also at the client's request flow out of my business as follows:

- Client requests I share information with another health professional e.g. GP or physiotherapist.
- Client requests I share information with a third party e.g. insurance company where they have been receiving treatment related to a claim they are making e.g. following a car accident.

In the above instance I will take all reasonable steps to ensure that:

- The request is from the client i.e. requesting identification and confirmation of known data to identify and authenticate an individual
- It is the most expedient option – wherever possible clients would be provided with their own data for onward sharing.
- Data is appropriately secure e.g. encrypted prior to being sent.

2. The personal data I hold, where it came from, who I share it with and what I do with it.

Information Asset Register

- I hold personal information about my clients that they have given me.
- This includes name, address, contact details, age, GP practice/name.
- I also hold health and wellbeing information about them which I collect from them at their first consultation to ensure treatment is safe and effective.
- I also hold relevant lifestyle information e.g. hobbies, levels of activity, stress levels and other factors which can impact pain and injury recovery.
- I hold information about each treatment that they receive from me.
- I don't share this information with anyone unless requested by the client to do so (see previous section).
- I use the information I have in order to inform my treatments and provide them with any appropriate advice within the realms of the treatment, my professional experience and qualifications.
- I also use contact details and any expressed interests e.g. sport or treatment specific such as back pain, to market to existing customers or former prospects with relevant content or offers. A separate consent will be sought for using data in this way. This consent can be withdrawn at any time and is entirely separate from consent to treatment.
- I keep all data for:

    a. claims occurring insurance: for which I am required to keep my records for 7 years after the last treatment
    b. children's records: for which I am required to keep my records until the child is 18 or beyond this where 7 years elapses after they reach the age of 18.
    c. registration with the ISRM and CTHC (for my work as a soft tissue and massage therapist).

3.The lawful bases for me to process personal data and special categories of data.

I process the personal data under:

- **Legitimate interest:** I am required to retain the information about my clients in order to provide them with the best possible treatment options and advice.

- **Special Category Data - Health Related:** I process under special category data, therefore the additional condition under which I hold and use this information is for me to fulfill my role as a healthcare practitioner, bound under the ISRM and CTHC Codes of Practice and Ethics.

4. Privacy Notice

Individuals need to know that their data is collected, why it is processed and who it is shared with. This information is included in my privacy notice and discussed at first consultation. Prior to consultation when a client books an appointment the privacy policy is emailed to them.

For individuals receiving pre or post event massage where a full consultation is not completed then only a name and signature is attained. In these instances the privacy policy and a shortened version is on display next to the sign in sheet prior to treatment and the therapist checks the client is happy to proceed on the basis their name is retained for 7 years or longer in the case of a minor.

I have written a privacy notice, and have ensured that the privacy notice includes all of the information included in the ICO privacy notice checklist at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed#table

5. Processes to recognise and respond to individuals' requests to access their personal data.

All individuals will need to submit a written request to access their personal data - either by email or by letter. I will provide that information without delay and at least within one calendar month of receipt. I can extend this period by a further two months for complex or numerous requests (in which case the individual will be informed and given an explanation).

I will identify the client using reasonable means, which because of the special category under which I process data, will be photographic ID. I reserve the right to ask for personal data or treatment data to be confirmed by the client prior to release if the identity of the applicant is in any doubt

I will keep a record of any requests to access personal data.

6. Processes to ensure that the personal data I hold remains accurate and up to date.

I will ensure that client information is kept up to date during our treatments, and will update client information as I am informed of any changes.

7. Schedule to dispose of various categories of data, and its secure disposal.

Once a year I will review my client information and will place dormant clients in a separate file. This will be assessed after 7 years and annually thereafter to ensure that data that is no longer required to be kept under GDPR is destroyed securely.

8. Procedures to respond to an individual's request to restrict the processing of their personal data.

If I receive a request to restrict processing of an individual's data then I will respond to this as soon as is practicably possible and no later than one month explaining that data will be retained but not used for marketing purposes which is the only scenario in which restriction is likely to be requested.

9. Processes to allow individuals to move, copy or transfer their personal data from one IT environment to another in a safe and secure way, without hindrance to usability.

Should clients wish their data to be copied or transferred I would work with the client to ensure that this is done in a way that was most appropriate for them - for example this could be an electronic summary of treatment received and progress made, copies of individual treatment records. I do not hold any treatment information electronically at present.

Where treatment has covered numerous sessions and is written in therapist shorthand which would not be understandable to the client a reasonable and proportionate admin fee may be requested to cover time spent documenting this in a client friendly way – this will be on a time and materials basis based on current treatment costs.

10. Procedures to handle an individual's objection to the processing of their personal data.

I will inform my clients of their right to object "at the point of first communication" and have clearly laid this out in my privacy notice.

11. Processing operations that constitute automated decision making.

I do not have any processing operations that constitute automated decision making and therefore, do not currently require procedures in place to deal with the requirements.

12. Data Protection Policy

This document forms my privacy and data protection policy and shows how I comply with GDPR.

This is a live document and will be amended as and when any changes to my data processing takes place, at the very least it will be reviewed annually.

13. Effective and structured information risks management

The risks associated with my data, and how that risk is managed is as follows:

- Theft of electronic devices - both have password locks on all electronic devices which are changed regularly and are not shared with anyone.
- Break in to office/treatment space - all my paper files are stored in a locked drawer in my house. No one else has the key but me.
- Theft of paper files while travelling – while travelling paper files for clients are kept on my person at all times and never left unattended in a car or similar.
- Event sign in sheets – At events sign in sheets are in public view at present as they also act as a queuing system. Only name is listed on this sheet and no other sensitive data. However consideration is being

given to how this process can be made more secure going forward e.g. sign in sheet held by therapist and not on view to the public with a separate system used for queueing e.g. raffle tickets.

-

14. Named Data Protection Officer (DPO) and Management Responsibility

Although not required to have a named DPO, as the sole employee I am the DPO and will ensure that I remain compliant with GDPR.

15. Security Policy

All my electronic devices are standard well known brands with industry recognised secure software.

16. Data Breach Policy

A personal data breach means a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

I understand that I only have to notify the ICO of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

Where a breach is likely to result in a high risk to the rights and freedoms of individuals, I will notify those concerned directly and without undue delay.

In all cases I will maintain records of personal data breaches, whether or not they were notifiable to the ICO.

Data Protection Policy created: 23rd May 2018

Data Protection Policy updated: 13/8/2019

This is a live document and will be updated as and when changes occur.

Date of Next Review: 13/8/2020

……

Signed: Sarah Maidment