Data Protection Privacy Policy

Sheena Hayward
Massage Therapist

A. The Data Protection Privacy Policy, fair processing notice and privacy statement

Sheena Hayward Massage Therapy ('we' 'our' or 'us') recognises our responsibility to comply with the EU's General Data Protection Regulation (GDPR) EU/2016/ 679 which regulates the use of personal data.

"Personal Data" is information about you which can be used alone, or combined with other information, to identify you personally and can include expressions of opinion about an individual. This does not have to be sensitive data; it can be as little as a name and address.

Our Privacy Policy must be read together with any other legal notices or terms and conditions available on other pages of our Website and it describes how we collect, use and otherwise handle "Personal Data" that we receive from you when you use our Website, correspond with us and use our services. It explains the circumstances in which we may transfer this to others.

It is our policy to keep our client lists up to date and for any bulk emails to be sent to one unidentifiable source eg info@ and for other recipients to be blind copied in to avoid disclosure of their email addresses which are private Personal Data.

.

We acknowledge that the Personal Data that you provide may be confidential. We will maintain the confidentiality of and protect your information in accordance with this Privacy Policy and all applicable laws. The law requires us to tell you about your rights in regards to processing and control of your Personal Data. We do this now by requesting that you read the information provided at **www.knowyourprivacyrights.org**

B. General Data Protection Regulations (GDPR)

The GDPR sets out high standards for the handling of Personal Data and protecting individuals' rights for privacy. It also regulates how Personal Data can be collected, handled and used. The GDPR applies to anyone holding Personal Data about people, electronically or on paper.

When dealing with Personal Data, it is our policy that our staff must ensure that:

- **Data is processed fairly, lawfully and in a transparent manner**

This means that personal information should only be collected from individuals if staff have been open and honest about why we want the personal information.

- **Data is processed for specified purposes only**

This means that data is collected for specific, explicit and legitimate purposes only.

- **Data is relevant to what it is needed for**

Data will be monitored so that too much or too little is not kept; only data that is needed should be held.

- **Data is accurate and kept up to date and is not kept longer than it is needed**

Personal Data should be accurate, if it is not it should be corrected. Data no longer needed will be shredded or securely disposed of.

- **Data is processed in accordance with the rights of individuals**

Individuals must be informed, upon request, of all the Personal Data held about them.

- **Data is kept securely**

There should be protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

C. Storing, and accessing data

We recognise our responsibility to be open with people when taking Personal Data from them. This means that we must be honest about why we need a particular piece of personal information.

We may hold Personal Data about individuals such as their names, addresses, email addresses and telephone numbers. These will be securely kept and are not available for public access.

Individuals have the right
*to have their data rectified if it is incorrect,
* the right to request erasure of the data,
*the right to request restriction of processing of the data and
*the right to object to data processing,

although rules do apply to those requests.

D. HOW, WHEN AND WHY DO WE COLLECT AND USE PERSONAL DATA?

GDPR Article 6 Lawfulness of processing

Each condition provides an equally valid basis for processing personal data.

1. Processing shall be lawful only if and to the extent that at least ONE of the following applies:-

(a) the data subject has given Consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is Necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is Necessary for compliance with a Legal Obligation to which the controller is subject;
(d) processing is Necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(f) Processing is Necessary for the purposes of the Legitimate Interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

1.<u>Legal grounds for collection of your Personal Data</u>

We will only collect, use, retain and destroy your Personal Data within Article 6 when:

• it is necessary for the performance of a task carried out in our Legitimate Interests within Article 6, in particular:

•responding to your queries;
• providing services and/or information to you;
•transmitting Personal Data internally for administration purposes;
•hosting and maintaining our Website;
•preventing and detecting fraud and other criminal offences; and/or
•ensuring network and information security,
* as required by law or any regulatory authority as long as, in each case, these interests are in line with applicable law and your legal rights and freedoms;
• where you have given Consent for processing your Personal Data for one or more specific purposes; and/or

• where this is necessary for compliance with Legal Obligations to which we are subject and /or
* where this is necessary for the performance of any contract with you.

Certain contact information about our therapists will be published on our website for contact purposes.

2.How we 'collect' your Personal Data

Contact Forms - we may collect your Personal Data which you provide when you fill in forms in correspondence / face to face with us. This may include, for example, your name, contact details (such as business and personal emails, telephone number and home address), and your personal preferences, choices and requirements specific to particular requests or services.

We may supplement the information that you provide, with other information that we obtain from our dealings with you. We would usually expect to keep a record of your contact details.

Where permissible under applicable local laws, we may combine Personal Data that you have provided to us, with other information that we already hold, or may come to hold, about you and which we have collected for tasks carried out as part of our Legitimate Interests.

We may also record (provided we have your prior explicit written consent) details of any disability, health needs (ie Special Categories of Personal Data) that you may have to enable us to ensure your safety.

3.How we 'use' your Personal Data

We may use any Personal Data that you provide to us in a way that is adequate, relevant, and not excessive:-

* where legally required or permitted for specific stated purposes made clear at the point of collection or on particular pages of our Website; and/or where we otherwise have legal bases under the GDPR for collection and use of your Personal Data, as explained in more detail above.

*Personal Data may also be disclosed to law enforcement, regulatory, or other government agencies, or to other third parties, in each case to comply with legal or regulatory obligations or requests.

If you choose not to provide Personal Data requested by us, we may not be able to provide you with the information and/or services you have requested or otherwise fulfil the purpose(s) for which we have asked for your Personal Data.

E. Children's privacy protection

We understand the importance of protecting children's privacy in the interactive online world. Our Website is not designed for or intentionally targeted at children of 16 years of age or younger. It is not our policy to collect or maintain intentionally any information (including photographs) about anyone under the age of 16 without the express specific written consent of the parent or guardian.

F. HOW LONG DO WE RETAIN PERSONAL DATA? WHEN IS IT DELETED?

It is our policy to retain your Personal Data for no longer than absolutely necessary and only for the length of time required for the specific purpose or purposes for which it was collected, after which it will be deleted.

However, on occasion we may be obliged to store some data for a longer time, for example, where a longer time period is required by applicable laws. In this case, we will ensure that your Personal Data will continue to be treated in accordance with this Privacy Policy.

We will store your Personal Data for whatever time period we consider reasonable in the circumstances; or as we are required to do by law or any regulatory authority; whichever is longest.

After Personal Data is not needed any more, or if the information is out of date, or if it has served its use and falls outside the minimum retention time of our document retention policy, it will be shredded or securely deleted from the computer.

We will only retain Personal Data of staff and clients for as long as is necessary:-
(a) for the purposes for which it was collected in the first place; or
(b) as is required by law or any appropriate regulatory authority ; or
(c) in order to establish, exercise, or defend legal claims.

G. HOW AND WHEN DO WE SHARE PERSONAL DATA WITH THIRD PARTIES?

1. Some services that we provide, require the involvement of third parties. We have carefully selected these third parties and have taken steps to ensure that your Personal Data is adequately protected.

2. Sharing within our organisation and authorities

Where you ask or indicate that we should do so, or where we are otherwise legally permitted to do so in accordance with this Privacy Policy, we may share your Personal Data (including any emails or correspondence to us) with such of our staff as need to see it. We may use the information you provide to us in relation to our administration.

When we intend to use your Personal Data for a new purpose, we will let you know about this.

3. Sharing with Service Providers

a) Unless otherwise provided in this Privacy Policy, we will not sell, rent or trade or make your Personal Data commercially available to third parties without your express written consent. We will only pass your Personal Data to others in accordance with:-

*this Privacy Policy,
* our own professional advisers and third party service providers who are bound by confidentiality codes, and
*when we are legally obliged by law or by any appropriate regulatory authority to disclose your Personal Data including, where necessary, for the purposes of preventing and detecting fraud, other criminal offences and/or to ensure network and information security

b) We will not normally share your Personal Data with any other organisation, however, some of our treatments may be provided by or held at premises of third parties and we may need to provide limited Personal Data to them to enable you to take part.

c) We will keep all information about you confidential at all times unless you tell us to release information, or we must release information by law or by any regulatory authority or we must release information because of the nature of the services that we are carrying out for you and other clients.

d) Personal Data may also be disclosed to other third parties in order to respond to your requests or inquiries, or where those parties handle information on our behalf.

e) In order to carry out work for you, we may need to collect information about you to pass to third parties (e.g. to other service providers) for the purposes of supplying services to you and others. This may involve the transfer of information outside the European Economic Area (“EEA”). We will let you know if we need to transfer your Personal Data to any third party service providers located outside the EEA. (eg “in the cloud”).

f) We may share your Personal Data with our third party service providers based in the European Economic Area ("EEA") whom we engage to process the information that we collect from you, and/or to host and maintain our Website, content or services, on our behalf and in accordance with this Privacy Policy.

g) Where we employ third party companies or individuals to process Personal Data provided by us (and not collected by them), they only use this Personal Data on our behalf and in line with our express written instructions and this Privacy Policy. Occasionally, we may need to appoint other organisations to carry out some activities on our behalf. These may include, for example, courier or call answering services. In these circumstances, we will ensure that your Personal Data is properly protected and that it is only used in accordance with this Privacy Policy.

H. **Derogations**

i) Despite paragraph G.3 (c), we may make documents and correspondence relating to your personal data available to the court or other authority as appropriate, or someone it has appointed, for it to assess a file or financial record.

.

Despite paragraph G.3 (c), we may ask an external typing company to type up letters and documents using your personal data.

Despite paragraph G.3(c), we may make details of your membership available to any current or any future insurers.

I . Anti-Money laundering regulations

The Anti-Money Laundering Regulations 2007 say we must, in many cases, gather evidence of the identity of those we deal with.

As a result, we may possibly do an independent computer identity check on you with another service provider and we may ask you to show us some form of personal or business documents (as required by these Regulations), including photo ID, to check your identity.

The service provider who carries out the check, if one is to be done, will record the fact that we have carried out a search. The service provider may also reveal your information to a Credit Reference Agency to confirm your identity. That Agency may keep a record of the search, but they will not carry out a credit check and your credit rating will not be affected. We use these third party search agencies and to obtain information about you for these purposes only.

J. Photographs of individuals and Feedback forms

Under 16's are dealt with separately below

Feedback forms will be sent to clients at SHMT's discretion

The person providing the feedback must have given express or implied consent to the processing of their feedback for publicity material and/or on the website before any part is published.

J.1. Adults

Posed photographs of a client for a press release or a marketing leaflet.

The parties in the photo must have given express or implied consent to the processing of their personal data for this press release and / or marketing leaflet purpose only. Not for ongoing PR unless that purpose is stated. We will need to keep consents under review and refresh them if our purposes or activities evolve beyond what we originally specified

Posed photographs of a client for putting on our website.

Have the parties in the photo given consent to the processing of their personal data for our website? We try to get specific Consent and to record it for this purpose only.

We need to give granular separate options to consent separately to separate purposes, unless this would be unduly disruptive or confusing. People may wish to consent to their information being used for one purpose but not another.

J.2.UNDER 16s

Photo ID of a parent consenting to his/her under 16 being photographed in treatment for our website section on eg how under 16 friendly we are.

Consent of the parent or guardian is needed and the photo ID of the parent or guardian will be deleted after the check on the parent or guardian.

K. SAFEGUARDING POLICIES FOR UNDER 16'S

SHMT has achieved professional accreditation that is up to date.

This can be viewed as evidence that SHMT has attained a certain level of safe practices as assessed by the awarding body.

SHMT has:-

• a named and contactable welfare officer (Sheena Hayward) responsible for the implementation of safeguarding under 16s.
* a policy and issues regarding the protection of under 16s
• procedures for dealing with complaints or concerns regarding poor practice, abuse or neglect
• written standards of good practice (ie a code of conduct/behaviour)
• a parental consent/emergency details form that must be returned to us.
• safe recruitment procedures for those working with under 16s that include: a clear job description, appropriate references, criminal records checks (eg DBS) for relevant posts and technical qualifications
• access to appropriate safeguarding (child protection) training for our staff

Signed parent's consent and emergency details

As part of your under 16's registration, parents or guardians are asked to complete a consent form. This should ask for emergency contacts, key medical information (allergies, asthma, etc.) and whether there are any other issues we need to know about, in order to help your under 16 get the most out of their therapy. Clients under the age of 16 must be accompanied at therapy by their parent or guardian who must give permission for the treatment to be performed and must co-sign the client's consultation / information form. The parent or guardian must be present in the room throughout the treatment

Recruitment of staff

All staff have been selected through a proper recruitment process. This should include interviews, references and Disclosure and Barring Service (DBS) checks –for staff working with under 16s.

Safeguarding training to be provided for staff

All staff should have up-to-date safeguarding training.

Health and safety

We have readily accessible guidance on first aid (and ideally a qualified first aider), and the following are available within our therapy premises:
• first aid box
• procedure for reporting and responding to injuries or accidents that occur within our premises
• arrangements for providing participants with appropriate medications (parental consent will be required for application of medication)
• that the therapy venues satisfy fire and other relevant regulations

If your under 16 needs help with using their medication, discuss and agree with us how these personal care needs will be addressed.

L. INTERNATIONAL TRANSFERS
The transfer of your Personal Data may involve your Personal Data being sent outside the EEA, to locations that may not provide the same level of protection as those where you first provided the information eg if your Personal Data is held by us on "the cloud".

However, we will only transfer your Personal Information outside the EEA:
• where the transfer is to a place that is regarded by the European Commission, or appropriate supervisory data protection authority, as providing adequate protection for your Personal Data ; or
• where we have put in place appropriate safeguards, for example by using a contract for the transfer which contains specific data protection provisions that have been adopted by the European Commission or a relevant supervisory data protection authority, or
• where you have consented to this, or
* there is another legal basis under GDPR's Article 6 on which we are entitled to make the transfer.

M. SECURITY
Our Website is hosted on servers in the UK or in the wider EEA. We take the security of your Personal Data seriously. We have strict procedures and security features in place to ensure that our paper and computer systems and databases are protected against unauthorised use, loss and damage and guarded against access by unauthorised persons.

We undergo periodic reviews of our security policies and procedures to ensure that our systems are secure and protected. However, as the transmission of information via the Internet is not completely secure we cannot guarantee the security of your information transmitted to or from us.

N. YOUR RIGHTS
If you wish to:
• access, confirm, correct, rectify, update, supplement, anonymise, block, restrict or delete your Personal Data ;
• object to our use of your Personal Data;
• if you have any questions about our processing of your Personal Data; or
• if you would like to transfer your Personal Data from us to another person or business,

please contact us.

We will provide you with all rights in relation to your Personal Data to which you are entitled under applicable law. If you are unhappy with the way that we have handled your Personal Data, you can make a complaint to the Information Commissioner's Office responsible for data protection in the UK. Contact details are typically available online, or alternatively you may ask us for assistance.

O. CHANGES TO THIS PRIVACY POLICY
We may change our Privacy Policy from time to time. When we change our Privacy Policy, we will publish the updated policy on our Website. Please check this Privacy Policy regularly.

Subject to applicable law, all changes will take effect as soon as we publish the updated Privacy Policy, but where we have already collected information about you and/or where legally required to

do so, we may take additional steps to inform you of any material changes to our Privacy Policy and we may request that you agree to these changes.

P. HOW TO CONTACT US

If you have any questions in relation to this Privacy Policy, or if you would like to contact us to exercise your rights as stated in this Privacy Policy, you may contact Sheena Hayward by email contact@sheenahaywardmassage.co.uk tel: 07392 232338

.

Q. Subject Access Request (S.A.R.) Procedure

We are aware that people have the right to access any Personal Data that is held about them. Subject Access Requests (SARs) must be submitted in writing (this can be done in hard copy, or email). If a person requests the above contact point to disclose any Personal Data that is being held about them, our SAR response will detail:

- How and to what purpose Personal Data is processed
- The period we tend to process it for
- Anyone who has access to the personal data

If a SAR includes Personal Data of other individuals, we must not disclose the personal data of the other individual. That individual's personal data may either be redacted, or the individual may be contacted to give permission for their information to be shared with the data subject.

This procedure is to be followed when an individual contacts us to request access to their personal information held by the Club. Requests must be completed within 30 days, so it should be actioned as soon as it is received. SAR's should be provided free of charge, however, we can charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive.

It is our policy that the steps below should be followed to action the request:

1. Is it a valid Subject Access Request?

a) The request must be in writing (letter, email, social media or fax).

b) Has the person requesting the information provided us with sufficient information to allow us to search for the information? (We are allowed to request for more information from the person if the request is too broad.)

2. Verify the identity of the requestor.

a) We must be confident that the person requesting the information is indeed the person the information relates to. We should ask for the person to attend in person with their passport/photo driving licence and confirmation of their address (utility bill/bank statement).

3. Determine where the personal information will be found

a) Consider the type of information requested and use the data processing map to determine where the records are stored. (Personal Data is data which relates to a living individual who can be identified from the data (name, address, email address, database information) and can include expressions of opinion about the individual's health)

b) If we do not hold any Personal Data, we will inform the requestor. If we do hold Personal Data, we will continue to the next step.

4. Screen the information

a) Some of the information we have retrieved may not be disclosable due to exemptions, however as a policy, legal advice will usually be sought by us before applying exemptions.

Examples of exemptions are:

- References given to us
- Publicly available information

- Crime and taxation
- Management information (restructuring/redundancies)
- Negotiations by us with the requestor
- Regulatory activities (planning enforcement, noise nuisance)
- Legal advice and proceedings
- Personal data of third parties

5. Are we able to disclose all the information?

a) In some cases, emails and documents may contain the personal information of other individuals who have not given their consent to share their personal information with others. If this is the case, the other individual's personal data will be redacted before the SAR is sent out.

6. We will prepare the SAR response (*using the template letters at the end of this document*) and will make sure to include as a minimum the following information:

a) the purposes of the processing;
b) the categories of personal data concerned;
c) the recipients or categories of recipients to whom personal data has been or will be disclosed, in particular in third countries or international organisations, including any appropriate safeguards for transfer of data;
d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;
e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
f) the right to lodge a complaint with the Information Commissioner's Office ("ICO");
g) if the data has not been collected from the data subject: the source of such data;
h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

We will be careful also to provide a copy of the personal data undergoing processing.

All SAR's will be logged to include the date of receipt, identity of the data subject, summary of the request, indication of whether we can comply, and the date information is sent to the data subject.

Sample letters:

Replying to a Subject Access Request providing the requested personal data

"[Name] [Address]
[Date]

Dear *[Name of data subject]*

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [subject]. We are pleased to enclose the personal data you requested.

Include the information in Article 6(a) to (h) above.

Copyright in the personal data you have been given belongs to SHMT or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] making a data subject access request for [*subject*]. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose [some/most] of the personal data you requested. [*If any personal data has been removed*] We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that [*if there are gaps in the document]* parts of the document(s) have been blacked out. [*OR if there are fewer documents enclosed*] I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt*].

Include the information in Article 6(a) to (h) above.

Copyright in the personal data you have been given belongs to SHMT or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.
Yours sincerely"

Replying to a subject access request explaining why we cannot provide any of the requested personal data

"[Name] [Address]
[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of [date] *or relevant to on-going or preparation for litigation. Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject. Advice will be taken whether a relevant exemption applies and if we are going to rely on the exemption to withhold or redact the data disclosed to the individual, then in this section of the letter we will set out the reason why some of the data has been excluded*.]
Yours sincerely

Sheena Hayward Massage Therapy