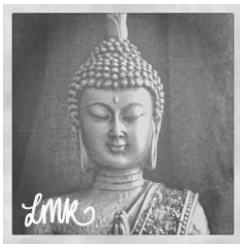
LMK

Complementary Therapist



Laura Kitto
Brewer Rd, Cliffe Woods
Rochester, Kent, ME3 8HS
: 07795 146117
: laura.kitto@hotmail.co.uk
: www.laurakitto.com

GDPR: Data Protection Policy

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

GDPR Registration
I have registered with the ICO and this is renewed automatically each year.

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 4 ways:

a. Via email messages to me from potential clients and clients that have my email address.
b. Via text messages to my mobile phone.
c. Via my website [web provider: wix.com]
d. Via Facebook Messenger and other social networking platforms.

It flows through my business via:

- My laptop - which I use at my work/home premises [password protected]
- My smart phone - everywhere I go [password protected]
- My paper file – which is at my work/home premises [lockable file]

The information does not flow out of my business.

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, and, where appropriate, age. I also hold health and wellbeing information about them which I collect from them at their first consultation.
- I hold information about each treatment that they receive from me.
- I don't share this information with anyone. However, please note, in line with Safeguarding protocols; in the event that there is an indication that a child or vulnerable adult may be at risk of harm, it is an obligation to report concerns to the necessary agencies.
- I use the information I have to inform my treatments and provide them with any appropriate advice within the realms of the treatment, my professional experience and qualifications.
- I keep all data for:

    a. claims occurring insurance: for which I am required to keep my records for 8 years after the last treatment
    b. law regarding children's records: for which I am required to keep my records until the child is 25, or if 17 when treated then until they are 26.
    c. registration with The Complementary and Natural Health Care Council (for my work as a Reflexologist): for which I am required to retain information for 8 years.

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 fulfil my role as a complementary therapy practitioner, bound under the CHNC and the FHT Confidentiality as defined in their Codes of Practice.

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 on my website and within any forms or letters I send to individuals, including at my first consultation with my client.

I have written a privacy notice for my website and for my clients, 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 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.

Once a year I will also have a wholesale review of all data.

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 each month 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.

As I only hold data in order to provide treatments, I cannot envisage a situation where I would receive a request to restrict their processing of an individual's personal data. However, if I do receive a request I will respond as quickly as possible, and within one calendar month, explaining clearly what I currently do with their data and that I will continue to hold their data but will ensure that it is not processed.

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.

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. This right is, however, included in my privacy statement.

12. Data Protection Policy

This document forms my 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.
As the only member of staff I believe that I have done an appropriate amount of research around the implications of the new GDPR, including taking heed of the advice and guidance provided by my professional membership organisations (CNHC for my work as a Reflexologist and FHT for my work as a Reflexologist and Reiki practitioner).

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 - all my paper files are stored in locked filing unit in my home. No one else has the key but me.
- Theft of paper file while at home - my home is fitted with a burglar alarm and CCTV.

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

As detailed in my risk assessment. I have also chosen my electronic equipment based on their industry record as having the most robust inbuilt protection possible.

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.

17. Disposal of Data in the event of incapacity/death

In the event of an unforeseen circumstance such as my sudden death or an event leaving me incapacitated my next of kin is nominated to securely dispose/shred client data.

Data Protection Policy created: 10 May 2018; This is a live document and will be updated as and when changes occur.
Date of Last Review: July 2022 [updates: amendment/addition to consultation form extracts on page 4 of this document.]
Date of Next Review: as and when amendments are required.

Laura Kitto
LMK Complementary Therapist, Brewer Road, Cliffe Woods, Rochester, Kent, ME3 8HS
Tel: 07795 146117
email: laura.kitto@hotmail.co.uk

LMK Complementary Therapist
GDPR: Data Protection Policy – Privacy Notice & Client Consent.

Prior to July 2022: The following statement is an extract from my paper consultation form which all clients are asked to sign* at their 1st appointment:

Privacy/Data Protection: I have been offered a copy of the therapist's Privacy Policy in line with GDPR, which is also available to view on their website. I understand that data will not be sold or shared with any third party [except in the case of a safeguarding concern]. I consent to my data being used to form the basis of a treatment and for no other purpose, and that the therapist may contact me in future by text, email, social media messaging platforms or telephone in relation to future appointments and for marketing purposes, if applicable. I have the right to change my mind and will notify the therapist accordingly.

From July 2022: The following statements are extracts from my online consultation form which clients are asked to complete & submit prior to their 1st appointment, or if they are a returning client who has not visited for over 1 year:

LMK Client Consultation Form

By Completing This Form, this helps Laura Kitto tailor therapies for each individual client. It is also a requirement by my insurance providers to obtain personal information in order to support the therapies I provide. PRIVACY NOTICE: As a Holistic & Complementary Therapist, providing therapies to help improve the wellbeing of clients, Laura Kitto (LMK) is required to note personal information about her clients. This information will be kept secure, and no personal data will be shared with 3rd party organisations. The only exception to data sharing is where there is a safeguarding concern relating to a child or vulnerable adult perceived to be at the risk of harm, in which case data may be shared with the necessary safeguarding agencies. Please see Data Protection Policy for full details of how your data is protected. (Available to view at www.laurakitto.com/information-policies)

☐ I am aware of the LMK's Privacy Notice & Data Protection Policy in line with GDPR, which is also available to view on their website. *

☐ I understand that LMK may need to contact me with regard to appointments using the contact information provided and I will notify LMK if I wish to opt out of receiving general update emails. *

Full Client Consultation Form is available to view on my website: https://forms.wix.com/f4cad18b-254a-4a45-b9ee-b5211ddebbdb:97686357-c62f-457a-841b-9f57e3b3362c