Documented Created: 24th May 2018
Date of Last Review: 24th May 2018
Date of Next Review: 24th May 2019

GDPR: Data Protection Policy: Caroline McWilliam

Caroline McWilliam (Operating as a Sole Trader)
20 Ransom Road
Woodbridge
Suffolk
IP124JU

Clinic:
20 Ransom Road
Woodbridge
Suffolk
IP12 4JU

www.carolinemcwilliam.co.uk

Policy Purpose

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

Policy Content

1.The data that I process and how it enters and moves through my business.

Data comes into my business in 4 ways:

a. Via telephone (mobile 07979 853867)
b. Via email messages to me from potential clients (PC), clients(C) and other health professionals that have my email address.
c. Via text messages (as above)
d. Via my website

Data is held on:

- My smart phone – which is PIN protected.
- My desktop computer – retained in my clinic, and is password protected.
- My paper files – retained in my clinic in a locked filing cabinet.

  Electronic files are backed up to secure on-line storage.

2. The personal data I hold, where it came from, who I share I 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 without your express consent.
- I use the information I have to inform my treatments, review progress, and provide clients 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 7 years after the last treatment

  b. registration with The Craniosacral Therapy Association (Code of Ethics), for which I am required to keep my records for 7 years after the last visit for most adults and up to 21 plus 7 years for most children; 15 years rather than 7 for adults or children who lack 'capacity'

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 rules set by professional bodies.Confidentiality as defined in their 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 in 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 filing system. This will be assessed periodically, 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 encrypted electronic summary of treatment received and progress made, copies of individual treatment records.

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 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 (CSTA and CTHa)

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 – they have password locks on all electronic devices which are not shared with anyone.
- Break in to clinic – The building is locked when empty. Notes are kept in a locked filing cabinet.

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

I have 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, within 72 hours of discovering it.

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: 24th May 2018
This is a live document and will be updated as and when changes occur.

Date of Next Review: 1st May 2019

……
Signed: Caroline McWilliam