Janet Dowling
clinical hypnotherapist

Policy and Procedures for Protection of Data and Privacy
Updated 26th May 2020

Contents

Janet Dowling
clinical hypnotherapist

Policy and Procedures for Protection of Data and Privacy
Updated 26th May 2020

Section A

Introduction

Data held by Janet Dowling Clinical Hypnotherapist (me) will be held lawfully and for the retention periods set out in section B of this policy document.

This document refers to:

- Visits to my website
- Social media communication
- Emails
- Phone numbers
- Text messages
- Written Documents
- Hardcopy case notes and files
- Database entries
- Spreadsheets
- Images
- Recordings
- Supervision notes

Aim and Purpose

The purpose of this document is to ensure that I have a framework that ensures the rights and freedom of individuals in relation to their personal data (Article 1) and adheres to best practice in the management of client information and business records.

This document sets out the way in which information collated by me is managed and ensures that any information collected;

- is the right information
- is in the right place
- at the right time
- with the right people
- for the right reasons

This is a live document and may be updated at any time to reflect changes in law or growth of the business, and therefore should be revisited regularly to check for any updates. I am fully committed to ensuring clients' privacy and data protection rights.

Janet Dowling is the named Data Protection Officer/Controller and Head of Janet Dowling Clinical Hypnotherapy.

Janet Dowling
clinical hypnotherapist

Policy and Procedures for Protection of Data and Privacy
Updated 26th May 2020

Protection of Data and Privacy for Janet Dowling Clinical Hypnotherapist's clients

1. I am registered with the ICO (Information Commissioner's Office) as I hold some client data (phone numbers and email addresses) electronically. Being registered has the advantage of regular emails from them outlining any new changes in policy so I can keep up to date. My ICO reference number is ZA195605

2. I have attended a live online CPD course about The General Data Protection Regulation delivered by Tania Taylor, of Clinical Hypnotherapy School as well as an hour long telephone conversation with the ICO (Information Commissioners Office) to clarify what is required for my practice. In addition, I have watched and attended several seminars on FB live and at networking groups. This training need will be updated when required.

3. Any changes to my business processes and/or operations will be planned and will comply with the framework to ensure any risks to personal and sensitive information are minimised.

4. Any data collected is for the purpose of providing a person-centred service to an individual client and to refine my marketing. I do not send out newsletters or promotional emails. I only contact clients in relation to their ongoing treatment with me, for example texts to remind them of appointments or emails transferring the MP3 recording.

5. The Caldicott Principles are used to provide guidance in best practice when handling personal data, alongside the ICO's Office Codes of Practice. (https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx)

6. All technology (Microsoft Office products including Outlook and Dropbox) used to store or facilitate information and communication is maintained according to this policy.

7. All records are identifiable, locatable, retrievable, and intelligible according to regulations set out by GDPR.

8. It is my responsibility to ensure that I allow time and resources to prioritise adhering to Data Protection Legislation in my business.

9. Any electronic devices where personal or sensitive, confidential information is held will be password protected. Individual documents (invoices or letters to other healthcare professional) stored electronically will also contain individual passwords. My laptop is encrypted as well as password protected.

10. Procedures have been put in place to ensure the General Data Protection Regulations are met. These can be found in Section C.

Policy and Procedures for Protection of Data and Privacy
Updated 26th May 2020

Section B

Privacy Notice: Use of information

In accordance with my data retention schedule there may be occasions when data is not destroyed due to ongoing investigation, ligation or enquiry. The data will be deleted upon confirmation that it is no longer required.

On some occasions anonymised personal data will be retained whereby a client has provided a testimonial for use on my website or printed literature (flyers, adverts, website). When data is non-identifiable GDPR law is no longer applicable. Non-identifiable means that if this data was left on a bus, no one, including the data subject would be able to identify that this data was relating to them.

Personal information is collated and stored in hardcopy in a locked filing cabinet behind a locked door. I save clients' names and phone numbers in my work phone which is password protected. If they have emailed me I will use their email address to reply to their email.

Under the General Data Protection and Retention (2018) legislation, regarding how personal data is processed, all individuals have;

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision-making including profiling.

Please note that I do not use automated decision-making tools, including profiling.

Third Party Service Providers

To support the service I provide I use several third party services

Website visitors
QBD is a third-party service that hosts my website, https://www.janetdowling.co.uk. QBD uses anonymised data to collect visitor information such as how long an individual remains on a page of a website.
QBD's privacy notice can be found here: https://www.quickbydesign.co.uk/privacy
I also use Google Analytics to collect information about what visitors do when they click on my website, e.g. which page they visit the most. Google Analytics only collect non-identifiable data which means I or they cannot identify who is visiting. I have chosen to keep the data for 38 months as this will allow me to track busy times of the year.
Google Analytics's privacy notice can be found here: https://policies.google.com/privacy

Emails
GoDaddy is a third-party service that hosts my email.
GoDaddy's privacy notice can be found here: https://uk.godaddy.com/agreements/showdoc.aspx?pageid=PRIVACY

Email contact through a third-party provider
Some clients make contact with me via my website contact form or through one of the associations I am a member of. I am listed on, and can be contacted through the following sites NCH (National Council for Hypnotherapy) and the Hypnotherapy Directory .

Facebook
I have a business Facebook page https://www.facebook.com/JanetDowlingClinicalHypnotherapy/ which is public. Anyone following me or liking the page can see who else is following me. Any comments posted on my posts are public. If clients message me via my business page Facebook also stores the information.
Facebook's privacy notice can be found here: https://www.facebook.com/privacy/explanation

Video Link therapy sessions
For therapy sessions via video link I use Zoom, Business WhatsApp depending on the client's preference.
Zoom's privacy notice can be found here: https://zoom.us/docs/en-us/privacy-and-security.html

Business WhatsApp
I use the Business WhatsApp app to send some clients the MP3 recording. Here is a link to their privacy statement:
https://www.whatsapp.com/legal/#privacy-policy

Bank Transfers
If a client chooses to pay by bank transfer (BACs) I request that they use their initials as the reference. I don't share my bank statements with anyone, including my accountant however using initials provides a level of anonymity as well as allowing me to identify who has paid. I bank with Santander.
https://www.santander.co.uk/personal/support/customer-support/legal-information

Card Payments
If a client pays by card I use the services of a company called SumUp. I have copied the pertinent part of their Privacy Policy below. Access to their full Privacy Policy is here.
https://sumup.co.uk/privacy/?_ga=2.85391577.1178106971.1549285810-183414184.1544790081
1.5 When you use our Services we collect information relating to your transactions including time, location, transaction amount, payment method and cardholder details.
6.1. SumUp is responsible for the security of cardholder data which is processed, transmitted and stored within our systems. To this end, SumUp is certified as compliant under the Payment Card Industry Data Security Standard (PCI-DSS). SumUp applies best industry practice to safeguard this sensitive data and to ensure that it operates in line with these requirements, and to this end SumUp undergoes annual audits to ensure that we continue to meet this high standard.

Retention Schedule

Personal data collected	**How long I keep it**	**How I dispose of it**
Initial enquires from potential clients usually involves them giving me their contact details – name, email, phone number	I write down the details and return their call/email within one or two days. If they make an appointment I enter their mobile into my phone. If not I keep the written number and name for up to 4 months before shredding it. With email correspondence I keep the email for up to 4 months before deleting it. If the email has sensitive information in it I write the email address down and delete the email after I've read it.	Shredded paper Deleted email from email account and also on Weebly Form Entries if contacted through website contact form
Client records including initial consultation notes and session notes. These include name, address, phone numbers, emails, information as to why clients have come to me, medical information that may be pertinent and doctors name and practice address.	In accordance with CNHC regulation, 8 years after final treatment session has ended. Child records should be held until after 25th birthday, or 26th birthday if aged 17 when treatment ends.	Shredded
Email (including sent items)	Delete once treatment is completed, MP3 is sent via WeTransfer and paper entries are taken for contact information. If no appointment is booked then delete after 4 months.	Delete from email account and also on Weebly Form Entries if contacted through website contact form.
Phone numbers held on work iPhone and iPad	Delete contact when sessions have been completed. If there is no formal end to the sessions then delete contact if not heard from them for 4 months. All entries to be deleted prior to decommissioning of mobile device or reissue of device	Delete on work iPhone
Tracking document	Indefinitely or earlier if consent is withdrawn	Individual client data deleted if a Right to Erasure Request is made
Written testimonials	Indefinitely or earlier if consent is withdrawn	Delete on websites and don't use on the next reprint of printed material

Recordings – video testimonials	Indefinitely or earlier if consent is withdrawn	Delete on all devices if requested
Images taken – for promotional material	Indefinitely or earlier if consent is withdrawn	Delete on all devices if requested and don't use on the next reprint of printed material
Waiting lists – paper copy	Annual review period every April, old waiting list destroyed and new waiting list written.	Shredded
Supervision records	To be retained while I am in service and until 8 years afterwards.	Shredded
Complaints	2 years from the complaint being resolved with guidance from associations.	Shredded
Right to Erasure Request	8 years from request being submitted and completed. Contact insurance and associations and ICO if request is made.	Shredded
Subject Access Request	8 years alongside session notes, or plus 2 years from case closure if request is made after 6 years of storing data. Contact insurance and associations and ICO if request is made.	Shredded

The *Information Owner Asset* is me, Janet Dowling, for all data. Hard copy data will be destroyed via a cross shredding machine owned by the me, electronic data will be permanently deleted.

In the event of an emergency, where I am unable to contact current clients about postponing their appointment, then my husband will ask a 'trusted professional' to contact clients using my work phone.

In the event of my death then my husband will ask a 'trusted professional' to contact my insurance company and associations for their advice and take responsibility of contacting current clients and destroying any relevant data in accordance to the advice given.

The **trusted professional** will be someone my husband knows that I have a strong professional relationship with, for example a fellow Solution Focused Hypnotherapist, my supervisor, a fellow education professional or health professional.

Policy and Procedures for Protection of Data and Privacy
Updated 26th May 2020

Data Processing

Lawful basis for processing data at Janet Dowling Clinical Hypnotherapist

As the data I process about clients is considered special category data and is required by me to provide my service as a clinical hypnotherapist and psychotherapist I do not require consent to hold clients' data to provide this service. Participating in my service, by attending more than one appointment, implies that clients agree with the Terms and Conditions provided to them at the start of sessions with me.

I do however require consent from clients for additional specific purposes

- Using contact details for sending reminders or rearrangements of appointments
- Using contact details to transfer my MP3 recording
- Using contact details to conducting videolink appointments
- Contacting other healthcare professionals

Description of processing
The following is a description of the way I processes personal information.

Reasons/purposes for processing information
I process personal information to enable the provision of hypnotherapy and psychotherapy, to maintain accounts and records and to advertise my services.

Type/classes of information processed
I process information relevant to the above reasons/purposes. This information may include:

- personal details such as name, address and contact details
- family, lifestyle and social circumstances
- goods and services – sending my MP3 through electronic transfer
- financial details – either on cheque, direct transfers or card payment

I also process sensitive classes of information that may include:

- physical or mental health details
- offences and alleged offences

I process personal information about:

- clients
- suppliers
- professional advisers
- supervisors

Section C
Data Breach

All personal and sensitive data held by me is held securely.

Hardcopy data is held securely in a locked cabinet behind a locked door. In the case of therapy sessions away from the main therapy room clients' notes will be kept in a locked bag either with me or in the therapy room.

Electronic data may be stored in the follow ways:

- On my passcode protected work iPhone and iPad and Microsoft tablet
- On my passcode protected and encrypted laptop
- In password protected individual files
- In password protected cloud storage Dropbox https://www.dropbox.com/en_GB/security#files

In the case of a data breach I shall comply with the regulations set out under Article 33 of the GDPR;

1. In the case of a personal data breach I shall *'without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual. Where the notification to the ICO is not made within 72 hours, it shall be accompanied by reasons for the delay.'*

2. Informing the data controller is not relevant for me as I am both the data controller and processor.

3. If I need to notify the ICO of a security breach I shall
(a) *describe the nature of the personal data breach including where possible, the approximate number of data subjects concerned and the categories* (e.g. sessions notes, phone numbers*) and approximate number of personal data records concerned;*
(c) *describe the likely consequences of the personal data breach;*
(d) *describe the measures taken or proposed to be taken by the* me *to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.*

4. *Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.*

5. I *shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.*

6. *In the event that a data breach will likely cause a risk to the rights and freedoms of client data,* I *must communicate the nature of the breach in clear, concise and plain language, to the client/s involved, without delay.*

7. *If a breach occurs but the* I have *gone to appropriate lengths to protect the data held on the client (e.g. password encryption of electronic files), or if the data controller has taken subsequent action to prevent the risk (e.g. immediately blocking a mobile device) then notifying the client will not be required.*

Subject Access Request
A Subject Access Requests (SAR) permits individuals to request a copy of their personal information.

A SAR must be acted upon within one month, at the most within two months, any longer and reasonable reason must be provided. There are no fees unless there is a disproportionate fee for sending out the information.

Application for SAR will be held alongside session records, unless application was made after six years of the end of treatment. In which case the SAR will be held for a further two years after closure of SAR. I will in the first instance contact my insurance company, associations and ICO for advice if a request is made.

A SAR request will include information I hold about clients, I will:
- give clients a description of it;
- tell clients why I am holding it;
- tell clients who it could be disclosed to; and
- let clients have a copy of the information in an intelligible form.

SAR requests should be put in writing to me. A response may be provided informally over the telephone with the client's agreement, or formally by letter or email. ***If any information held is noted to be incorrect an individual can request a correction be made to their own personal information.*** This should be made in writing to me.

Right to Erasure
Any person may put in a request for their personal data to be removed (the 'right to be forgotten' or the 'right to erasure'). I am a member of CNHC (Complementary and Natural Healthcare Council) which require that I keep client notes for 8 years. So in the event of a Right to Erasure Request I will, in the first instance, contact my insurance company, associations and ICO for advice.
Hard copy data will be shredded using a cross shredding machine owned by the me and any electronic data will be permanently deleted. The client will be notified of the completion.
The request for deletion of data and the confirmation of completion will be held securely until eight years after the request was made.

Complaints
I strive to the meet the highest quality standards when processing personal and sensitive data. Complaints can help identify areas for improvement and therefore I would welcome any concerns clients may have.

These Information Governance Policy documents were created to be as transparent and understandable as possible. It will not be completely exhaustive of all aspects of data collection. For further information about a specific process, please contact Janet Dowling Clinical Hypnotherapist.

If you feel you would like to make a complaint about how your personal and sensitive data is handled by Janet Dowling Clinical Hypnotherapist you can contact Janet Dowling Clinical Hypnotherapist directly. In the event that Janet Dowling Clinical Hypnotherapist cannot resolve the complaint satisfactorily contact can be made with the Information Commissioners Office on 0303 123 1113.

Safeguarding Privacy of Clients

Everything we talk about during the sessions is strictly confidential between my client and me. To ensure I am doing my job effectively and that I have the right support, I may discuss elements of the sessions with my supervisor. During these discussions I do not disclose any details that may identify my clients to my supervisor or anyone else in the supervision group.

If I see a client outside of a session I will smile but will not engage in any further conversation to ensure their confidentiality. I request, that in order to ensure the success of their treatment, that they refrain from discussing their treatment with me outside of their sessions.

I will not add clients as a Facebook friend. However, some friends on Facebook become clients and will remain as a friend unless they unfriend me.

After sessions are complete I will not contact clients unless they contact me first. From experience, some clients like to share their successes, sometimes many months after the sessions are finished and I love to hear them. If a client does get in touch with me I will respond positively and ask if they would be happy for me to use it as a testimonial. If they don't reply I don't ask again.

Children and Teenagers

I require consent from the parents or legal guardians of all children and teenagers age 16 and under, except in special circumstances. I follow the NHS guidance regarding consent for children and young people for these special circumstances which is based on being Gillick competent. I would always seek advice from my professional associations and supervisor before taking on a client under the age of 17 without their parents' or guardians' consent.

I provide children and teenagers with a separate Terms and Conditions document as well as their parents or guardians with the regular one I use. This is so that my clients, whatever age, are informed about what to expect from sessions as well as the data I keep and why.