Privacy Policy Checklist

What to provide or explain if you are a 1:1 practitioner or have a newsletter or website

About you / your business:

☐ The name and contact details of your business.

☐ *The name and contact details of anyone in your business that a customer may wish to deal with directly (e.g. a representative or, if you have hired one, your data protection officer*

About the data you collect and why:

☐ What you are using the data for.

☐ The lawful basis you have for doing that.

☐ The legitimate interests (i.e. if one of your bases for keeping and/or using the data is 'legitimate interests' you also have to say what those are).

☐ Where else you get their data from, and what that data is

☐ Exactly how long you keep the data for.

About what you *share* and why:

☐ Who you send or may send their data out to (if you do) – naming the specific person or business, or naming the 'type' of recipient such as 'the police'

☐ The details of transfers of the personal data to any third countries or international organisations (if applicable).

Customer rights:

☐ All the rights your customer has*.

☐ The right to withdraw consent (if the data usage is based on consent).

☐ The right to lodge a complaint with a supervisory authority (Professional association, the ICO).

*There are eight rights. Not all of these may apply in your situation. The main seven are explained in the webinar and shown on the template privacy policy. Further details can be found in the private Facebook Group

When your business gets bigger you may also need to declare these other details, for example if you one day design an insurable practitioner training and are required to keep an active database of registered/qualified practitioners

☐ The details of whether individuals are under a statutory or contractual obligation to provide their personal data

E.g. you may make it part of their *contract* as a qualified practitioner to keep you updated on current address, contact details, insured status. This will allow you to respond if one of their clients contacts you as the 'supervisory authority' (to complain), and also allow you to see if someone has not been in practice for a year or more (e.g. if continuous practice and cpd are requirements to retain status)

☐ The details of the existence of automated decision-making, including profiling

E.g. If there is a practitioner test that is run online and marked automatically – you may also want to give contact details for any 'real person' specifically dealing with that, if it is not you.

When you are finally at this level, the eighth customer right will also come into force. That relates to their rights to do with automated decision making and automated personal profiling (and when that method can and cannot be used).

Here is a sample Privacy Policy. There are many ways to lay this information out, as long as you cover everything that is in the checklist above and this is just an example. Don't forget to look at the GDPR compliant privacy policies turning up on websites that you value and to take ideas from those.

In this following example I have not just listed customer rights, but also gone into detail. You can just as easily give less info and simply say what the right is and how to activate it (i.e. both verbally or in writing).

Areas for alteration to suit your own business are highlighted in yellow.

If you like this layout it is also being given to you as a separate word document for ease of editing. On the word document version feel free to delete whole sections if they do not apply or to add more, as you wish.

Privacy Policy

This is the privacy policy for Name, trading as Business name

And as the following website(s) and social media identities:

Websites / FB Page names etc

Contact details:

Postal address

email

There are two sections to the following information:

1. About your personal data – the type of data that is collected or used, including when, how and why
2. Your rights – all the ways that you can control what happens with your data

About your personal data:

When you make an enquiry

The name and contact details you give and the content of your message(s) are retained for three reasons:

1. By your consent
2. As part of a 'contract' (only while we communicate)
3. For legitimate business interests – for good business practice I keep tabs on who has made contact before, the types of questions asked etc

When you make an online purchase as a single purchase, a membership or subscription

This is a contract for services. Your contact details are dealt with as above (consent, contract, legitimate reasons) – also these, your purchase history and the payment details (sent to me from Paypal or Stripe) are retained for six years beyond the end of the contract for legal reasons – accounting law.

When you attend a workshop or training

All of the above applies. I also keep record of your attendance, your certificates earned etc on the legal bases of both contract and legitimate interest – so that I can confirm your certificate status / reissue certification if required, also so that I can send you updates or offers which may be of specific interest to you as an attendee/graduate.

When you work with me 1:1

Client work is different. Dependent on the work, you may wish (or need) to provide personal details of a sensitive nature.

As an intake form this data is retained in printed or handwritten format and include your contact details and where appropriate, signature. The sensitive nature of such documents will generally be in relation to health or medical history.

As session notes these are scant memos handwritten by me for the purpose of fulfilling our contract and keeping tabs on the work during the session and from one week to the next, filed separately with only initials and date as identifiers so that no other person may connect these details alone to your personal identity.

In both cases I am required by law to retain these records for six years after the completion of our contract – or in the case of a minor, from six years beyond the date of their eighteenth birthday.

Other data sources:

Incoming data is also received from my website host Weebly, when you contact me through my site, also from Paypal or Stripe, when you make a purchase and Skype or Zoom when we hold an online meeting or client session.

I may also, with your clear consent or request, receive information from another practitioner or therapist as part of a referral. In such a case you may be unaware that the consented data transfer has taken place, I will therefore inform you of receipt within 28 days.

Sharing your data

Your privacy is important and I do not sell your data. I do not share your data except as outlined here and by your consent or under the law.

When working together, I may, with your clear consent or request, give out elements of your personal information to another practitioner or therapist as part of a referral.

In continuation of current UK law on confidentiality I also retain the right and in some cases the legal requirement to breach confidentiality, to inform an authority such as the police or your GP of impending harm or illegality.

Your Rights

The GDPR sets out clearly what your rights are. It also lays out deadlines for a reply and other rules which are reproduced for your information at the bottom of this section.

Right to be informed

You have the right to be informed about the collection and use of your personal data. This is a key transparency requirement under the GDPR.

I must provide you with information including: my purposes for processing your personal data, my retention periods for that personal data, and who it will be shared with. This 'privacy information' is provided above.

I must provide you with privacy information at the time I collect your personal data from you, in other words it has to be available to you before you fill in a form or hand over your data such as your email address.

If I obtain your personal data from other sources, e.g. by referral or from the payment service provider your selected, I must provide you with privacy information within a reasonable period of obtaining the data and no later than one month.

There are a few circumstances when I do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it.

The information I provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language. Therefore if there is anything you do not understand, please get in touch.

Right of access

You have the right to access your personal data and supplementary information. This allows you to be aware of and verify the lawfulness of the processing.

You are entitled to confirmation that your data is being processed, access to your personal data, and
other supplementary information as provided in this privacy notice

Right to rectification

You have the right to have the data your personal data corrected if it is incorrect, or completed if it is incomplete.

Right to erasure

You may request, verbally or in writing, to have your data erased. This is also commonly known as 'the right to be forgotten'. This right only takes effect when:

- Your personal data is no longer necessary for the purpose for which it was originally collected or processed,
- you withdraw your consent when the sole legal basis to hold this information is your consent,
- There is a legitimate interest in processing this data, which does not override your request
- processing/analysing of the personal data was for direct marketing purposes and this is the use you object to
- your personal data was processed unlawfully without a proper legal basis
- There is a legal obligation to comply with your request; or
- If the personal data was processed to offer information society services to a child.

Right to restrict processing

You have the right to request the restriction or suppression of your personal data. In other words you want to stop the data being used but keep it on file.

In this case your personal data cannot be used and can only be stored unless:

- you give your consent;
- it is for the establishment, exercise or defence of legal claims;
- it is for the protection of the rights of another person (natural or legal); or
- it is for reasons of important public interest.

Right to data portability

This allows you to obtain and reuse your personal data for your own purposes across different services. It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. Doing this is meant to enable you to take advantage of applications and services that can use this data to find you a better deal or help you understand your spending habits. In general this rule exists for data held by big service providers, such as your call history or insurance or gas bill history. The right also only applies to information you have provided.

If, as a private client you wish to carry a copy of your case notes or other sensitive data to another practitioner or other mental, physical or spiritual health service, these may be provided to you or to the nominated service provider, on request, as an encrypted and password protected document.

Right to object

Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

Your objection must be made on grounds relating to your particular situation.

Once you object your data can no longer be processed, unless

- there are demonstrably compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

You may complain directly to me using the contact details above. If you find the outcome unsatisfactory you are then able to object or complain to:

Name and contact details of ICO , professional association or insurer

You may of course also exercise your right to legal action.

Timelines:

You can claim a right verbally or in writing.

A response should come without delay and at least within one month of receipt. The time limit is calculated from the day after you make the request (whether the day after is a working day or not) until the corresponding calendar date in the next month.

I aim to respond within 28 days.

Exceptions:

When you request access to your data, a copy must be provided free of charge. However, you can be charged a 'reasonable fee' when a request is:

- manifestly unfounded or excessive, particularly if it is repetitive, unless that's because I failed to respond; or
- for further copies of the same information (that's previously been provided).

Handy hint: When issuing a privacy policy, keep a note in the footer of creation date and version number. This helps clients to realise that you do sometimes review and update your processes. It also helps you to make sure that if you update your printed Privacy Policy you are using the same version on your website too!

Intake forms:

Intake forms vary wildly – we are complementary therapists filling the space between mainstream counselling, health and wellbeing and pastoral care and some of us veer toward the life and business coaching model. Each intake form will therefore be unique.

There are a wide variety of professional layouts to be found here: (Google search results)

More checklists:

Below are three more checklists to help you look at the ways that you collect data, and to help you set up ways to respond to clients making an objection.

Remember that you may only have one or two paths for incoming data and that you may never come across an objection, particularly if you have a good intake form.

1. Data Audit questionnaire
2. ICO's checklists for managing consent
3. Handling objections questionnaire

You will need this information from the ICO website:

If you refuse to comply with an objection you must

"inform the individual without undue delay and within one month of receipt of the request. You should inform the individual about:

- the reasons you are not taking action;
- their right to make a complaint to the ICO or another supervisory authority; and
- their ability to seek to enforce this right through a judicial remedy.

"You should also provide this information if you request a reasonable fee or need additional information to identify the individual."

"You can extend the time to respond to an objection by a further two months if the request is complex or you have received a number of requests from the individual. You must let the individual know within one month of receiving their objection and explain why the extension is necessary."

Data audit questionnaire

Why do you use personal data in your business?

Who do you hold information about?

What information do you hold about them?

Who do you share it with?

How long do you hold it for?

How do you keep it safe?

What are your processing contracts with EU and non-EU processors?

What if anything needs updating on your current privacy policy?

ICO's checklists for managing consent:

Asking for consent

☐ We have checked that consent is the most appropriate lawful basis for processing.

☐ We have made the request for consent prominent and separate from our terms and conditions.

☐ We ask people to positively opt in.

☐ We don't use pre-ticked boxes or any other type of default consent.

☐ We use clear, plain language that is easy to understand.

☐ We specify why we want the data and what we're going to do with it.

☐ We give separate distinct ('granular') options to consent separately to different purposes and types of processing.

☐ We name our organisation and any third party controllers who will be relying on the consent.

☐ We tell individuals they can withdraw their consent.

☐ We ensure that individuals can refuse to consent without detriment.

☐ We avoid making consent a precondition of a service.

☐ If we offer online services directly to children, we only seek consent if we have age-verification measures (and parental-consent measures for younger children) in place.

Recording consent

☐ We keep a record of when and how we got consent from the individual.

☐ We keep a record of exactly what they were told at the time.

Managing consent

☐ We regularly review consents to check that the relationship, the processing and the purposes have not changed.

☐ We have processes in place to refresh consent at appropriate intervals, including any parental consents.

☐ We consider using privacy dashboards or other preference-management tools as a matter of good practice.

☐ We make it easy for individuals to withdraw their consent at any time, and publicise how to do so.

☐ We act on withdrawals of consent as soon as we can.

☐ We don't penalise individuals who wish to withdraw consent.

Handling objections questionnaire

How will you handle an objection?

How do (can) objections be submitted?

When does the right to object apply?

What is your policy for recording objections you receive verbally?

When can you refuse an objection?

What information must you give to the individual along with your refusal?

On your privacy notice / privacy policy, is the right to object explained clearly, under it's own heading, separate from (not mixed in with) other information on rights?

Apart from in the privacy notice, when else should you or could you inform people of their right to object?

How will you make sure you reply to an objection within one month, including (if successful) erasing the objectionable information?

What steps will you take and methods will you use to erase, suppress or stop the processing of personal data?

What circumstances mean you can legally extend the time limit to more than one month?