

Judy Blee
Counsellor & Supervisor

Accredited Professional Registrant Membership (PNCPS Acc.), Accredited CYP Therapist NCPS
BSc, PGCE, Post Grad.Dip.Psychology (GMBPsS), Adv.Dip.Couns, Adv. Specialist Dip. CYP & supervision



Data Protection & Privacy Policy 2026

As an NCPS Registered and Professional Accredited Counsellor/Psychotherapist I am also registered with the Information Commissioners Office (ICO) as follows:

Date registered 01 April 2019 valid to 31 March 2027

1. Legal Framework

As such there is a lawful basis for me to hold and process your personal details as this is legitimate for my work. This policy has been developed with regard to relevant UK data protection legislation, statutory guidance and recognised good practice. This includes the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and the Data (Use and Access) Act 2025, together with relevant safeguarding and information sharing guidance.

Where information is shared for safeguarding purposes, it also has regard to Keeping Children Safe in Education 2026 and Working Together to Safeguard Children and statutory information sharing guidance.

I will process personal information lawfully, fairly, transparently, and securely, and this policy will be regularly reviewed to reflect changes in legislation, regulatory guidance, and organisational practices.

2. What data am I collecting from/about you? What will I use it for?

I collect information about my clients, supervisees and students in a number of different ways. I ask for contact and other referral information when you first approach me and use this information to help provide a service to you; further the work we do together; and keep records of our communications. When you make payments to me I need information to help me administer these payments, including your name, address, email and telephone numbers.

When I am working with clients, supervisees, or students, in case an emergency arises during a session, I keep an additional/emergency contact name and telephone number. I also keep the name of your GP and their contact details, however I will only use this information where absolutely necessary and usually after consultation with you.

At the end of each session I make brief notes, to record what happens in our collaborative work together, and so that I can provide a safe, ethical service. The notes include details of what you would like to gain from therapy and they may be used in my own clinical supervision sessions, but they are encrypted and you cannot be identified by them.

3. Are there any circumstances where my data might be shared?

It is very unlikely that I will share your data with others, and I will definitely not sell it or use it for unethical purposes. The only exceptions to sharing data are listed below. In all these situations I would contact you to discuss this beforehand (unless I deemed this to increase risk to you or someone else).

- Where I am obliged to break confidentiality and share information by a court of law, because there is a risk of serious harm to you, or to the safety of others, or I am expected to do so by my professional association (National Counselling and Psychotherapy Society NCPS), in order to represent myself
- Where I am required to comply with Safeguarding legislation or Child and Vulnerable Adult Protection, because children or vulnerable adults are involved and at risk, I might need to contact your GP, the emergency, or social services
- Where matters of Trafficking, Money Laundering, and Terrorism legislation are involved

HOWEVER

- None of your personal data will be collected while you are visiting my website, in accordance with Data (Use and Access) Act 2025
- None of your personal data will be transferred overseas, or to any other destination, unless I am under a legal obligation to do so
- No Generative AI, or other transcribing or recording software is used on my website; during my therapy sessions with you online (I use Google Workspace for Business and Google Meets for video conferencing and data processing); on the telephone (my work mobile); or during face to face sessions
- No recordings are made from any of my online, telephone, or face to face sessions with clients, supervisees or students

4. How will I store your data?

All records that I store on my computer or mobile phone are encrypted and password protected. Your telephone number and email address may be kept on the mobile phone I use for work, but you cannot be personally identified from these records. The paper records and session notes I keep are kept securely in lockable filing cabinets in my office and filed under a coded system.

5. How long will I store your data, and how will I dispose of it?

I will keep your session notes for 6 years following the end of our work together, in accordance with guidelines suggested by my insurance company. Your personal contact details will be shredded or deleted within 12 months of our work ending.

6. What happens if you have been referred via another organisation?

If this organisation has policies which differ from mine I will comply with their policies as well as my own, as far as possible, although they may have given me more information than I would normally collect, for example your place of work and a reference number. I require this information in order to successfully invoice the organisation, as they need to recognise your case. This information is usually contained in an email which I will delete once the organisation has reimbursed me for our work together.

7. Do I have a right to see the information you hold? How can I get access to it?

Yes you do. If you ask me for the information that I hold about you I am legally bound to send you the information, free of charge, within 30 days of your request. I will make sure you are in control of your information and you can ask me to stop using it whenever you wish.

I will ensure that if you request printed or verbal information from me, I will only send or give that which is relevant to our work together and the services I provide. I will supply this information by post, email or telephone, depending on your expressed preferences.

Can I make a complaint to you about data protection breaches?

Yes you can. Because I run a small business I also act as Data Protection Officer. If you are not happy with the way I have collected, used, stored, shared or retained your personal information the law states that I must:-

- Give you a way of making a data protection complaint against me, either via email to judyblee@devontherapyrooms.co.uk, telephone to 07930 079504 or through my website www.devontherapyrooms.co.uk
- Where possible you should include your name, contact details, what has happened, which therapy intervention is concerned, what you would like me to consider, and any other relevant supporting information
- I will aim to acknowledge receipt of a data protection complaint within 5 working days but if this is not possible for any reason, I will acknowledge it within 30 days of receiving it
- I will make appropriate enquiries, investigate fairly and proportionately, and keep you informed
- Once my enquiries are complete, I will let you know the outcome of your complaint without undue delay, as well as any action taken
- Information about making a complaint is also available from the ICO and you can complain directly to them at: The Information Commissioner's Office,

www.ico.org.uk, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.
Telephone 0303 123 1113.

Any actual or suspected personal data breaches must be reported, without delay, to the Data Protection Officer. Examples include; information sent to the wrong person; loss of device or paper record; unauthorised access to an account; inappropriate access to an operating system; accidental disclosure of therapy; health or safeguarding information; or a cyber incident.

I will contain and assess the incident; protect affected people; record what happened and the action taken; notify affected people, where legally required; report the breach to the ICO, where legally required; and take action to reduce the risk of recurrence. Where a breach is reportable to the ICO, it will be reported without undue delay and where feasible within 72 hours of my becoming aware of it.

Our Contract/Agreement and Consent

Once we agree to work together, we draw up a written contract or agreement for this, which we both sign. As part of this process you consent to me using your data along the lines described in this policy.

The agreement explains that I will treat your personal details with care, respect and according to the legal framework outlined in this policy. If at any point you do not wish me to use your data in the ways I have described above, it is unlikely that I will be able to continue working with you.

Details of my Privacy and Data Protection policy are available on my website.