Privacy Policy and Privacy Notice

Destination Counselling

Policy owner and data controller: Jane Brown, Counsellor | BACP membership number: 408149 | ICO registration number: ZB613773

Effective date: 30 October 2026 | Next review due: 30 October 2027

This notice explains how I collect, use, store and share personal information when I provide individual and couples counselling online to adults aged 18 or over who are physically in the UK during sessions. It also explains the choices and rights available to you.

1. Who is responsible for your information

Jane Brown, trading as Destination Counselling, is the data controller for the personal information described in this notice. I am a sole practitioner.

Contact me about privacy, your records or your rights:

Jane Brown | Destination Counselling | Address: (available on request)

Email: destinationcounselling@outlook.com | Phone, text or WhatsApp: 07417 424379

2. What information I collect

Depending on how you contact me and the service you use, I may collect:

- identifying and contact details, such as your name, email address, telephone number and emergency contact details;
- appointment, availability, payment, cancellation and other service-administration details;
- information you share in counselling, including health and wellbeing information, personal history, relationship information, and brief notes relevant to our work;
- information needed for online-session safety, such as your current UK location area and callback number, and, where an urgent risk requires it, your precise location;
- your GP's name, practice and contact details, which I ask for and store solely for safeguarding purposes; information about other people that you share with me, including a partner, child, young person or adult at risk, where it is relevant to counselling or safeguarding;
- communications with you, including appointment emails, texts or WhatsApp messages, and, if you choose email counselling, the email messages and responses that form that service;
- payment information and transaction status from website payments through Stripe and direct bank transfers through Tide. Tide may receive payer and banking details, payment amount, date and reference information associated with a transfer; the exact details depend on what is transmitted by the sending bank;
- technical and account information generated when you use Zoom, my website or related online services, such as device, connection, account or transaction data.

I do not record Zoom counselling sessions. Please do not send information requiring an urgent response by ordinary email, text or WhatsApp. These channels are for arranging or managing appointments, not for counselling or emergencies.

3. Where information comes from

I normally collect information directly from you during an enquiry, booking, counselling session, payment or communication. In couples work, I may receive information from either partner. I may also receive limited information from a person you ask me to contact, a referrer, a supervisor, an

emergency contact or a safeguarding or other professional service. Where information comes from someone else, I will explain its source and use where appropriate and lawful.

4. Why I use information and the legal basis

I use personal information only for purposes connected with providing and managing counselling, protecting confidentiality and safety, and meeting professional or legal responsibilities. Depending on the purpose, I rely on one or more of these legal bases:

- Article 6 lawful basis: I process your personal information because it is necessary to arrange and provide the counselling service you have requested.
- Legal obligation: to keep or disclose records where the law requires it, including applicable financial and tax records.
- Legitimate interests: to run and protect my counselling practice, maintain proportionate professional records, respond to complaints, protect people from serious harm, and establish or defend legal claims. I consider your interests and rights when relying on this basis.
- Vital interests or another applicable legal basis: where necessary and legally permitted to protect someone's life or safety, including an urgent safeguarding situation.

Counselling may involve special-category information, such as information about your health, sex life or sexual orientation. In addition to the Article 6 lawful basis described above, I rely on your explicit consent under Article 9(2)(a) of the UK GDPR to process this information for counselling and to keep appropriate counselling and related safeguarding records. I ask for and record this consent separately in the Working Agreement; it is separate from your agreement to receive counselling. You may withdraw your consent at any time by contacting me. Withdrawal does not affect processing already carried out, or information I must retain or may process under another applicable lawful basis and Article 9 condition. In a separate legal or emergency situation, I may rely on another applicable legal basis and condition where permitted or required.

5. How I use and protect counselling information

I keep brief notes relevant to our work, together with appropriate appointment and service records. I ask for and store your GP details solely for safeguarding purposes. I will use those details only where a safeguarding concern makes it appropriate and lawful to do so, and will share only information that is necessary. Where it is appropriate and safe, I will discuss any proposed contact with you first. Paper records are stored in a locked place. Electronic records are held in a secure, password-protected folder. Access is limited to me and to people or service providers who need information for a legitimate purpose.

I discuss my work with my supervisor, to support safe and ethical practice. I use thoroughly anonymised information where practical. I share identifiable information with my supervisor only where you have agreed or there is an appropriate legal or ethical basis, and I limit what is shared.

My clinical will appoints my supervisor, as my executor. She has agreed to act in this role and is bound by the confidentiality arrangements agreed with clients. If I become unable to contact clients or die, she may use the minimum information necessary to contact them and help them consider alternative arrangements. She may access client information only to the extent necessary for these agreed duties and where she has lawful and secure access.

If you attend as a couple, information shared in a joint session is generally part of the shared work. Each partner has individual privacy rights, and joint attendance does not give either person automatic access to all information about the other. I will assess requests for personal information

individually and consider the other person's rights and the confidentiality arrangements in the Working Agreement.

6. When I may share information

I do not sell your personal information. I may share information, limited to what is necessary, with:

- Zoom, to hold online sessions and provide its technical services;
- Stripe and Tide, to take and administer website payments and direct bank transfers, and CLC Digital UK, which runs my website;
- my email, telephone, messaging and secure-storage providers, to communicate with you and keep records;
- my supervisor or, where relevant, my clinical-will contact, in the circumstances described above;
- my professional indemnity insurer, legal or professional advisers, where needed to obtain advice, manage a complaint or claim, or protect my practice;
- emergency services, safeguarding services, regulators or other authorities where disclosure is required or permitted by law, or is necessary to address a serious risk of harm.

I will normally discuss a proposed disclosure with you first where it is appropriate and safe. I may need to share information without asking you first where the law requires or permits it, or where telling you could increase risk or prejudice an investigation. The limits of confidentiality are also explained in the Working Agreement and Safeguarding Policy.

7. Online services and transfers outside the UK

I use the services listed below to provide counselling, communicate with clients, manage orders and payments, and store records. CLC Digital UK manages my WordPress website and website tools on my behalf and acts as a processor for that website information; I am the controller and decide how it is used. Depending on the provider, information may be processed in the UK, the EEA (including Ireland, Germany and the Netherlands), the United States, and other regions used by Apple iCloud for WhatsApp backups. This list describes possible provider locations; it does not mean every provider handles every category of information in every location. UK transfers to EEA destinations may be covered by UK adequacy regulations. For restricted transfers not covered by adequacy, safeguards may include the UK International Data Transfer Agreement (IDTA) or the UK International Data Transfer Addendum to EU Standard Contractual Clauses. Google may rely on the UK Extension to the EU–US Data Privacy Framework where applicable. Providers describe security protections such as encryption in transit and at rest; these controls do not by themselves identify a transfer location or legal transfer mechanism. The specific hosting locations, subprocessors and security configuration for CLC Digital UK's website service have not yet been confirmed. I do not record Zoom counselling sessions.

Service providers and information they may process:

Provider / purpose	Information it may process	Storage, security and provider links
Website — CLC Digital UK: Manages my WordPress website and hosting, with Google Analytics and Google Search Console installed.	CLC Digital UK can technically access contact-form entries and purchase details. Website hosting and security logs may include IP addresses, browser and device details. Google Analytics and Search Console provide visitor, usage and search-performance information. Google says Analytics does not log or store IP addresses from UK users.	CLC Digital UK acts as my processor when managing the website tools on my behalf. I am the data controller and decide how information is used. The website cookie notice offers Accept, Reject and Preferences; there is no personalised advertising. Google's published information describes global processing and says Google may rely on the UK Extension to the EU–US Data Privacy Framework or standard contractual clauses where applicable. CLC still needs to confirm the website hosting provider and locations (including backups, logs and support access), its subprocessors and the data each can access, the transfer mechanisms applying to the website service, and whether website data are encrypted in transit and at rest. The general location list in section 7 does not confirm CLC-specific hosting locations.
Business bank — Tide: Receives direct bank transfers for counselling fees, including payments made by students.	Banking and transaction details associated with the transfer, which may include the payer's name, sending-bank details, amount, date and payment reference, depending on what is transmitted.	Tide processes and stores information needed to receive, administer and record the transfer under its banking arrangements. Provider information: Tide privacy notice Tide: Tide's privacy notice says data are stored in the UK or EEA and may be transferred to vendors or affiliates in India and the United States. Tide says it uses adequacy arrangements or contracts to safeguard those transfers.
Video sessions — Zoom: Provides online counselling sessions.	Name or account details, session time, device and connection information, and technical data.	Sessions are not recorded. Provider information: Zoom Privacy at Zoom | Meetings privacy data sheet Zoom: Zoom says personal data may be transferred outside the UK/EEA/Switzerland. Its published safeguards include the UK Extension to the EU–US Data Privacy Framework and standard contractual clauses or another lawful transfer mechanism, as applicable.
Payments — Stripe: Processes website payments.	Payment-card details and transaction information; I receive the information needed to administer payment and confirm transaction status.	Stripe processes card details under its own arrangements. Provider information: Stripe Privacy Centre (includes international transfers) Stripe: Stripe says personal data may be processed in countries where it, its service providers or payment partners operate, including the United States. Its published safeguards include the Data Privacy Framework and the UK International Data Transfer Addendum or other applicable transfer mechanisms.
Backup storage — Apple iCloud: Stores the WhatsApp chat backup associated with my business mobile.	WhatsApp chat history and any media included in the encrypted backup, together with account and device information needed to provide iCloud.	The WhatsApp backup is end-to-end encrypted and password-protected, as configured. The backup is stored in the iCloud account linked to my business mobile. Provider information: Apple Privacy Policy | iCloud data security Apple: UK personal data may be transferred to or accessed by Apple affiliates worldwide; Apple says such data are generally stored by Apple Inc. in the United States and UK transfers are governed by standard contractual clauses. The precise location of this account's WhatsApp backup is not shown in the information available to me.
Email — Microsoft Outlook.com: Used to arrange appointment details, provide email counselling, and receive client order confirmations.	Email addresses, message contents and attachments, including email-counselling messages and order confirmations.	Copies of email-counselling correspondence that I retain are anonymised and saved in the password-protected OneDrive folder described below. Order confirmation emails are also stored securely in that folder. Provider information: Microsoft Privacy Statement Microsoft online-services DPA (if applicable): Microsoft DPA Microsoft: Microsoft's privacy statement says personal data may be stored or processed in the user's region, the United States and other jurisdictions where Microsoft or its service providers operate; it describes legal safeguards for international transfers. The specific region and terms for this Outlook.com account are not confirmed here.

Provider / purpose	Information it may process	Storage, security and provider links
Messaging — WhatsApp regular app: Used for appointment-related messages.	Phone numbers, message contents, delivery information and service/account data.	I use the regular WhatsApp app on my password-protected business mobile, which is not linked to another device. Chat backups are enabled with WhatsApp end-to-end encryption and password protection. The cloud account used for backups is iCloud linked to my business mobile. Provider information: WhatsApp UK Privacy Policy (includes transfers) WhatsApp: WhatsApp says it uses Meta infrastructure and data centres worldwide, including in the United States and Singapore. Its UK privacy policy describes adequacy arrangements for some transfers and UK transfer mechanisms, including the UK Addendum/IDTA and standard contractual clauses, for others. The WhatsApp backup in iCloud is end-to-end encrypted and password-protected, as configured.
Calls and SMS — Lyca Mobile (using the EE network): Used for client phone calls and text messages.	Phone numbers, call or message routing information, and SMS contents.	The handset is my password-protected business mobile. Provider information: Lyca Mobile privacy policy | EE privacy policy Lyca Mobile: Lyca's UK privacy notice identifies technical services in India and customer-service providers in Morocco and the Philippines. It says it uses contractual safeguards under applicable UK/EU data protection rules. The details of any EE network processing are subject to the relevant provider arrangements.
Electronic records — Microsoft OneDrive: Stores electronic client records in a password-protected folder associated with my Destination Counselling Microsoft account.	Electronic records, including anonymised copies of email-counselling correspondence and client order confirmations, as well as other counselling or safeguarding records.	The folder is not shared with anyone. Access is limited to me through my business account. Provider information: Microsoft Privacy Statement | Microsoft Products and Services DPA Microsoft: Microsoft's public information describes global processing and transfer safeguards. Business OneDrive data-at-rest location can depend on the Microsoft 365 tenant's provisioned region; the specific account type and location for this folder have not been confirmed here.

Before I enter your personal information into an AI or other digital tool, I will assess the tool's suitability, how it handles and stores information, and the risks to confidentiality. I will explain the proposed use, its benefits, risks and alternatives, and obtain your informed consent before entering your information. I remain responsible for professional decisions and will not delegate them to AI.

Your agreement and acknowledgment

I will give you this notice before or when I collect your personal information. I will explain the foreseeable limits to confidentiality, including supervision, safeguarding or legal disclosures, and the use of digital services that may collect or process information. I will ask you to confirm that you have received the notice and record your agreement to these confidentiality arrangements in the Working Agreement.

8. How long I keep information

I normally keep counselling records, including brief session notes and relevant service communications, for five years after our work ends. Safeguarding records are kept for five years after our work ends. After that, I securely destroy them unless a particular record must be kept longer to meet a legal obligation, deal with a complaint or claim, or protect someone's safety.

Financial and payment records are kept for the period required by tax and accounting law. Complaint information is kept for as long as needed to investigate and respond, and in line with my record-retention arrangements and any legal or claims requirements. Routine messages that are not

relevant to the work are not kept longer than necessary; where a message contains information needed for the counselling record, I may retain the relevant information there.

9. Your data-protection rights

Depending on the circumstances and the legal basis, you may have the right to ask for access to your personal information, correction of inaccurate information, deletion, restriction of processing, or a copy in a portable format. You may object to processing based on legitimate interests. Where I rely on consent, you may withdraw it. These rights are not absolute and may be limited where the law allows, including to protect another person's confidentiality or where information must be retained.

A request to access or change personal information is separate from a service complaint. I will respond within the time required by law. Contact me using the details in section 1. The current ICO guidance on rights is available at ico.org.uk

10. How to complain about my handling of your information

If you are concerned about how I have handled your personal information, please contact me first so I can investigate and respond. You may also complain to the Information Commissioner's Office (ICO), the UK supervisory authority, at ico.org.uk. My ICO registration number is ZB613773. My Complaints Policy explains the practice complaint process.

11. Changes to this notice

I will review this notice at least annually and when my services, data practices or applicable law change. I will give clients the current version before or when I collect their information, and draw attention to material changes..

12. Further information

The following independent guidance may be useful: ICO: the right to be informed and BACP: confidentiality and privacy