CHERRY BLOSSOM THERAPY

Privacy notice for clients and families

Final version 3.0 | Effective 3 November 2026 | Next review 3 November 2027

Cherry Blossom Consulting Ltd trading as Cherry Blossom Therapy | Company number 16479968
Sarah Musselwhite | 07311 473976 | cblossomtherapy@gmail.com
https://cherryblossomconsulting.co.uk

This notice explains how Cherry Blossom Consulting Ltd trading as Cherry Blossom Therapy uses personal information to arrange and provide psychotherapy and play therapy for people aged 4 to 24. It applies to clients, parents, carers, referrers and people who pay. We will explain it accessibly to children and young people. It covers the therapy service; website cookies and marketing, if used, need their own accurate information.

1 Who is responsible

Cherry Blossom Consulting Ltd, company number 16479968, is the data controller. Sarah Musselwhite is the contact for privacy questions and rights requests: cblossomtherapy@gmail.com or 07311 473976. Preferred correspondence is by email.

The company and practitioner hold separate ICO registrations. Cherry Blossom Consulting Ltd: ZC057834, expiring on 6 December 2026. Sarah Musselwhite: ZA840588, expiring on 6 January 2027. The company is the controller for the private-practice service described here; Sarah is the contact for privacy matters and handles records on the company's behalf.

2 Information we use and where it comes from

We use identity and contact details, date of birth, safe communication preferences, referral information, parental responsibility and relevant legal authority, attendance, agreements, billing and funding information. Clinical information may include assessment findings, session notes, therapeutic artwork where necessary, health and developmental information, accessibility needs, family circumstances, medication, risk assessments, safeguarding referrals and correspondence.

Some information is special category data, such as health, ethnicity, religion or information about sex life or sexual orientation. Safeguarding information may also include allegations, offences or criminal records. We collect only what is relevant; we do not routinely ask for complete medical or criminal histories.

Information comes from the client, parents or carers, referrers, schools, GPs, social care and other professionals where it is lawful to receive it. If someone else supplies information about you we explain this as required, subject to lawful safeguarding and other exceptions. Please tell us if information is inaccurate or if contact details are unsafe.

3 Why we use it and the legal basis

Arranging and delivering the service and managing payment: Article 6(1)(b), where processing is necessary for a contract with you or steps you request before it. Where a parent or agency contracts and the client is a different person, Article 6(1)(f), legitimate interests in providing a safe therapeutic service and appropriate administration, is used where justified after considering the client's rights. We do not assume the parent's contract is the child's contract.

Clinical assessment, therapy and records: we use necessary health information to assess and provide therapy under Article 9(2)(h), with the confidentiality safeguards in Article 9(3), Data Protection Act 2018 Schedule 1 paragraph 2 and section 11. Information is handled under the applicable legal duty of confidentiality in the therapeutic relationship. We record why these conditions apply. Consent to taking part in therapy is distinct from the legal basis for processing health information.

Safeguarding: the Article 6 basis depends on the purpose and applicable law. Article 6(1)(c) applies to an actual legal obligation, not every safeguarding concern. Otherwise a justified legitimate interest, or a recognised legitimate interest where the statutory conditions apply, may be appropriate. Special category information may be processed under Article 9(2)(g) with Schedule 1 paragraph 18 where necessary to protect children or individuals at risk and the conditions for processing without consent are met. Other conditions, such as health care or vital interests where the person cannot consent, apply only where their own requirements are satisfied.

Legal claims and complaints: justified legitimate interests or an applicable legal obligation support necessary processing; Article 9(2)(f) may apply to special category data needed for actual or prospective legal claims or legal advice. Tax and company accounting obligations support retention of necessary financial information under Article 6(1)(c). They do not require keeping all therapy content.

Criminal offence information: where necessary, we identify an Article 6 basis and meet Article 10 and a relevant Data Protection Act Schedule 1 condition, such as safeguarding under paragraph 18. We record the condition and apply the additional safeguards. We do not treat Article 9 alone as authorisation to process criminal offence data.

Optional sharing or other optional uses: where we rely on consent, we explain the specific purpose, information and recipient and obtain valid consent, including explicit consent for special category data where needed. You can withdraw it for future processing by contacting us. Withdrawal does not make previous lawful processing unlawful or require deletion of records we need to keep on another lawful basis. We will not change the legal basis merely to defeat a withdrawal.

4 Who may receive information

We agree routine updates and liaison with the client or lawful decision maker. Depending on need, lawful basis and confidentiality, information may be shared with a clinical supervisor, treating professionals, children's or adult social care, police, courts, insurers, legal advisers, relevant professional bodies and commissioners. Funding or referral does not give unrestricted access to clinical information. We verify the requester's identity and authority and share the minimum needed.

We may disclose without permission where required by law or a valid court order, or where necessary and proportionate under a lawful safeguarding or public interest justification. We normally discuss this first unless unsafe, prohibited or likely to prejudice an investigation. We do not report every disclosure of crime automatically. The Safeguarding Policy explains the forthcoming child sexual abuse reporting duty and how commencement and exceptions will be checked.

Clinical supervision uses anonymised or minimised information wherever possible. Identifiable material is used only where necessary and protected. Any separate company arranging therapy or hosting sessions has its own responsibilities; we clarify whether it acts as a controller or processor before sharing.

5 Storage and service providers

Sarah keeps records in a mixture of paper files and a clinical reporting application and is responsible for day-to-day handling. The company is the controller for its private-practice records, with Sarah managing the records on its behalf. We use appropriate physical and electronic security and restrict access to those who need it. Relevant providers may process information on the company's behalf under required contractual and confidentiality safeguards.

Clinical application providers are recipients of personal information where needed to provide secure record storage and clinical reporting. Please contact us for information about the provider used for your records, storage locations, backup retention and any international transfer safeguards. Any restricted international transfer must have a lawful transfer mechanism; you can ask for information about the safeguards and how to obtain a copy.

We will explain the actual digital systems and obtain informed agreement before personal data is entered into digital or AI tools, in line with professional requirements; this is distinct from the UK GDPR lawful basis. We do not use generative AI to process identifiable client information. We do not use solely automated decisions with legal or similarly significant effects about clients. This notice does not authorise session recording, AI transcription, uploading identifiable clinical information to generative AI, marketing or use of client work for publicity. Any proposed use needs a separate assessment and transparent information before it happens.

6 How long information is kept

Our clinical record retention schedule is as follows: for therapy ending before 18, until the 25th birthday, or 26th birthday if aged 17 when that course of therapy ended; for therapy ending at 18 or over, 7 years after the end of that course. An ongoing course crossing age 18 uses the adult end date rule, while any linked earlier child records due to be retained longer are not destroyed prematurely.

These are practice periods, not universal statutory minimums. Safeguarding concerns, complaints, legal proceedings, a preservation request, ongoing risk or an insurer's specific requirement may justify a documented longer period. Changes to limitation law, including child sexual abuse claims, must be considered individually; they do not mean all records should be held forever. We review records at the due date, minimise unnecessary material and record any extension and next review.

Unsuccessful referrals are normally reviewed for deletion 12 months after closure unless risk, a complaint or another recorded reason justifies longer. Administrative duplicates are deleted when no longer needed. Necessary company accounting records are generally kept for 6 years from the end of the relevant financial year, longer where law requires. Complaint records use the relevant clinical period where linked to care, with a documented review of any additional need. Paper and electronic information is securely destroyed when its retention period ends, subject to any lawful preservation hold. Backup copies remain protected and expire through the provider's backup cycle. Retention decisions take account of applicable law and the current insurance policy; where a longer period is required, we document the reason and review date.

7 Your information rights

You may ask for access, correction, erasure, restriction, or object where the relevant basis permits. Portability applies to qualifying automated processing based on consent or contract. Rights have conditions and exemptions; we explain any restriction and complaint route. You can make a request verbally or in writing. We verify identity proportionately and normally respond without charge within one calendar month, explaining any lawful extension or permitted pause in time.

The rights belong to the client, including a child. A parent may act with the child's authority or where lawful to act on their behalf; parental responsibility alone does not guarantee access. We consider the child's understanding, wishes, confidentiality, third party information and applicable exemptions, including serious harm provisions where relevant. We do not routinely disclose a child's therapy notes to resolve a family dispute.

You do not have to provide optional information. Without essential contact, consent, risk and clinical information we may be unable to assess or provide safe therapy; we explain what is needed and why. You may decline optional liaison without losing other rights.

8 Complaints and breaches

You can raise a privacy complaint by email or phone using the details above, or ask for an accessible form. We aim to acknowledge within 5 working days and in all cases within the applicable 30 day statutory limit. We investigate appropriately, keep you informed and communicate the outcome without undue delay; our target full response is 20 working days. A data rights request has its own legal timetable and is not delayed by the complaints process.

You may complain to the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/ or 0303 123 1113. We explain the independent route if the complaint concerns the practitioner. There is no charge to complain.

We record and assess personal data breaches promptly. Where notification is legally required, we notify the ICO without undue delay and, where feasible, within 72 hours of awareness, and inform affected individuals without undue delay where the breach creates a high risk, subject to lawful exceptions.

9 Updates

We review this notice annually and when services, law or providers change. Material changes are explained to clients where required. This notice is effective from 3 November 2026.

Document owner Sarah Musselwhite for Cherry Blossom Consulting Ltd. Effective 3 November 2026. Next scheduled review 3 November 2027, or sooner after relevant changes or incidents.

Sources and review

Official and professional sources supporting this policy are listed below. Use the live source for later changes. Local links give current reporting instructions and forms.

Data Protection Act 2018 as amended
ICO guidance on special category processing conditions
ICO notice on the data protection complaints duty
Crime and Policing Act 2026 Part 5 Chapter 2 and Schedule 12
Government implementation update dated 6 November 2026
PTUK Ethical Framework and good practice guidance
BACP Ethical Framework 2026 effective from 3 November 2026
Holistic Insurance Services published record keeping guidance
ICO registration and data protection fee guidance
Data Protection Act 2018 section 11 on confidentiality safeguards
ICO explanation of controllers and processors