Privacy Policy

Thrive Physiotherapy, including the Sapphire Children's Therapy service
Version 2.2 · Issued November 2026 · Next review August 2027
ICO registration reference ZB928406I

1. About this policy

When you use Thrive Physiotherapy you trust us with your information. This policy explains what we collect, why, what we do with it, how long we keep it, and what rights you have. It applies to clients and service users, parents and carers, people who contact us through the website, employees, and self-employed associates.

Data controller. Thrive Physiotherapy is the data controller for the information described in this policy. Thrive Physiotherapy is a trading name of Stephanie Clarke, operating as a sole trader. The Director performs the data controller function and is the named data protection lead. Our therapists, associates and therapy assistants process personal data under the Director's instruction and under the terms set out in this policy.

Regulatory registration. Thrive Physiotherapy is registered with the Information Commissioner's Office. Registration reference ZB928406I.

How to contact us about your data. Email hello@thrivephysiotherapy.org.uk, or write to us using the postal address available on request. We ask that data protection enquiries come by email where possible so that we have a dated record of your request.

Our legal framework. We process personal data in accordance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, and our professional obligations under the HCPC Standards of Conduct, Performance and Ethics.

2. Information we collect

On initial enquiry

- Contact details: name, address, telephone numbers, email address
- Details relevant to the enquiry: date of birth, relevant diagnoses, reason for contact
- Referral source, for example self-referral, GP, solicitor, case manager, school, local authority

For children and young people aged 0 to 25

- Parent or guardian details and a description of the family unit
- Educational placement details
- Pre-natal, birth and post-natal history
- Developmental information: milestones, feeding, communication, physical, sensory and learning profile
- Medical information: relevant illnesses, medications, relevant family history
- Reports from other professionals, including paediatricians, occupational therapists, speech and language therapists, psychologists, audiology, CAMHS and social care
- Education, Health and Care plans, individual education plans, school reports and progress notes from education staff
- Safeguarding history or concerns

For adult clients

- Contact details, medical history relevant to physiotherapy, GP and consultant details
- Reports from other healthcare professionals
- Safeguarding concerns, where relevant

Assessment and treatment records

- Assessment forms, standardised outcome measures, clinical notes, treatment plans, progress notes and discharge summaries
- Reports: EHCP, expert witness, medico-legal and tribunal reports
- Photographs and video, only where separate written consent has been given
- Correspondence: emails and records of telephone conversations. We use email for any communication about a client's care. Text messages are used only for appointment arrangements, such as times and changes. Where anything relevant to a client's care is said by text message or telephone, a note of it is added to the clinical record

Financial records

- Name of the bill payer and the client, invoices, receipts, records of payment, and bank details where these are provided to us
- Card and online payments are taken through Stripe. We receive the payer's name, email address, the amount, the date and the last four digits of the card. We never see or store full card numbers or security codes; these are held by Stripe.

Employee and associate records

Where we engage employees or self-employed associates we collect contact details, DBS certificate confirmation, HCPC registration, qualifications, references, right to work evidence, bank details and professional indemnity insurance details.

Website and online forms

- **Contact and enquiry forms.** We collect the name, email address, telephone number, enquiry type and message you provide. Submissions are processed by Formspree and forwarded to our inbox.
- **Feedback form.** Our client and family feedback form is hosted on Google Forms and responses are collected in a Google Sheet. We ask only for the information shown on the form. Feedback is used to improve the service, and is not published with your name attached unless you have agreed to that separately.
- **Website analytics.** We use Cloudflare Web Analytics to count page views and understand which pages are used. This service sets no cookies and does not track you across websites. It does process your IP address and browser user agent to distinguish one visit from another. No profile is built about you and the data is not used for advertising.
- **Cookies.** Our website sets no cookies. It does not use local storage, session storage, advertising tags or cross-site trackers. Because nothing is stored on your device, no cookie consent banner is required.
- **AI assistant.** We do not use an AI assistant to handle enquiries, and no part of your contact with us is processed by one. The chat panel on our website displays a message inviting you to get in touch and sends nothing anywhere. Should we introduce an AI assistant, we would complete a data protection impact assessment and update this policy before it went live.

3. Where our information comes from

Most personal data is provided by the client, or by a parent or person with parental responsibility for children. Where an adult lacks capacity within the meaning of the Mental Capacity Act 2005, information may be provided by carers, attorneys, deputies or professionals acting in that person's best interests.

Information may also reach us from schools and colleges, medical professionals, solicitors, case managers, local authorities and allied health professionals. Where we receive information about you from a third party we expect that party to have a lawful basis for sharing it, and we will tell you what we have received if you ask.

4. Our lawful basis for processing

For personal data we rely on:

- **Contract, Article 6(1)(b).** Processing necessary to deliver the service you have engaged us for.
- **Legal obligation, Article 6(1)(c).** Compliance with our regulatory, tax and record-keeping obligations.

- **Legitimate interests, Article 6(1)(f).** Running and administering the practice, including website analytics, recruitment and responding to enquiries. Where we rely on legitimate interests we have considered the effect on you and you may object at any time.
- **Consent, Article 6(1)(a).** Where we ask for consent, for example to share information with a named third party, or to use photographs or video.

For health and other special category data we rely on:

- **Health or social care provision, Article 9(2)(h)**, read with Schedule 1 Part 1 paragraph 2 of the Data Protection Act 2018. This is our main basis for clinical records.
- **Explicit consent, Article 9(2)(a)**, where processing falls outside the provision of care, for example use of images for teaching or marketing.
- **Legal claims, Article 9(2)(f)**, for expert witness and medico-legal work.
- **Substantial public interest, Article 9(2)(g)**, read with Schedule 1 Part 2 paragraph 18 of the Data Protection Act 2018, for safeguarding children and individuals at risk.

Automated decision-making. We do not make decisions about you by automated means and we do not profile you. All clinical decisions are made by a qualified physiotherapist.

5. How we use your information

- To provide physiotherapy assessment, treatment and ongoing care
- To produce clinical reports, including EHCP, expert witness and medico-legal reports
- To communicate with you about appointments and care
- To liaise with other professionals involved in your care, with your consent
- To deliver moving and handling training, risk assessments and other organisational services
- To process payments and maintain financial records
- To meet our professional, legal and regulatory obligations
- To respond to enquiries made through our website
- To recruit and manage employees and associates
- To understand which parts of our website are used, in aggregate

We do not sell your data. We do not use clinical information for marketing. We do not send marketing emails to clients unless they have asked to receive them.

6. How long we keep your information

Record type	Retention period
Clinical records, children and young people	Until the 25th birthday, or the 26th birthday where treatment ended at age 17
Clinical records, adults	8 years from the date of last contact or discharge
EHCP reports and tribunal documentation	Until the young person's 25th birthday
Expert witness and medico-legal reports	8 years from conclusion of the case, or longer where the instructing party requires it
Financial records, including payment records	6 years from the end of the financial year. Stripe also keeps its own payment records for the periods its legal obligations require.
Enquiries that did not proceed to assessment	12 months, then deleted
Website form submissions held by the form processor	12 months, then deleted from the processor's archive

Record type	Retention period
Employee and associate records	6 years from the end of employment or contract
Training attendance and competency records	6 years from the date of training
Website analytics	Aggregate counts only, retained for 6 months by the analytics provider. No individual record is created.

Where a record is subject to an investigation, complaint, safeguarding process or actual or likely litigation, we retain it in its original form until that matter is concluded, and then apply the period above.

Retention periods reflect the Records Management Code of Practice 2021 and the limitation periods that apply to clinical negligence claims, including the rule that a child's limitation period does not begin until their 18th birthday.

7. Who we share your information with

We do not share your personal information except in the circumstances below.

With your consent. We may share information with GPs, consultants, schools and colleges, local authorities, case managers and social care teams where you have agreed to it. For medico-legal work, information is shared with the instructing party as set out in the instruction.

For safeguarding. We will share information without your consent where we believe a child, young person or adult at risk is at risk of harm. We do this in accordance with the Children Act 1989 and 2004, the Care Act 2014 and local multi-agency safeguarding arrangements. Wherever it is safe to do so we will tell you that we are doing it.

Where the law requires it. We will disclose information where we are required to by law, by regulation, by our regulator, or by order of a court or tribunal.

Our data processors

These organisations process data on our behalf, under written terms that restrict them to acting on our instructions.

Processor	Data processed	Purpose
Google (Google Workspace)	Email, documents, clinical records, calendar	Business email, file storage and record keeping
Google (Google Forms and Sheets)	Feedback responses	Collecting client and family feedback
Formspree	Website enquiry form submissions	Receiving and forwarding website enquiries
Netlify	Website content. No client records. Server logs including IP address.	Website hosting
Cloudflare	IP address and browser user agent	Website analytics and content delivery
FreeAgent	Client or bill payer name, contact details, invoice amounts and dates	Invoicing, bookkeeping and tax returns
Stripe	Payer name, email address, payment amount and date, card details	Taking card and online payments through payment links
Starling Bank and Mettle (provided by NatWest)	Payment and invoice records	Business banking. Card payments taken through Stripe are paid into our Mettle account.

Stripe processes payments on our instructions. It also acts as an independent controller for some purposes of its own, such as fraud prevention and meeting its legal and regulatory obligations as a payment provider. Stripe's own privacy policy, at stripe.com/gb/privacy, explains that processing.

We review this list whenever we change a supplier and at each annual review of this policy.

Transfers outside the United Kingdom

Some of our processors are based in, or store data in, the United States. This applies to Formspree, Netlify and Cloudflare, and may apply to Google, Stripe and FreeAgent depending on the service. For UK businesses, Stripe's contracting entity is Stripe Payments Europe, Limited, in Ireland, which the UK recognises as providing adequate protection; data may then pass to Stripe, Inc. in the United States. FreeAgent is a UK company; its hosting providers store data in the UK, the European Union and the United States.

Where personal data leaves the UK we rely on one or both of the following safeguards:

- The UK extension to the EU-US Data Privacy Framework, where the receiving organisation is certified under it
- The International Data Transfer Addendum to the European Commission's standard contractual clauses, incorporated into our contract with the processor

Clinical records are held in Google Workspace with data residency and access controls applied. No clinical record is sent to a processor other than those named above. You may ask us for a copy of the relevant transfer safeguard.

8. Consent

Before an initial assessment, clients, or parents and carers where relevant, are given this policy and asked to complete a consent form. The form covers consent to assessment and treatment, the collection and storage of personal and health information, sharing with named third parties, and photographs or video where applicable.

Consent is recorded, dated and kept with the clinical record. You may withdraw consent at any time by telling us in writing. Withdrawing consent does not affect processing that has already taken place, and it does not override our safeguarding duties or our obligation to retain a clinical record of care we have already provided.

9. Photographs and video

Photographs and video are never taken without separate, specific written consent. Consent for clinical use, for use in teaching a client's own care team, and for use in marketing are asked for separately, and you may agree to one and not another.

Images are captured straight into the secured record system, so that no copy is left in a therapist's phone photo library or personal photo backup. They are filed with that person's own record, are accessible only to the therapists involved in their care, and are held in systems owned by the practice rather than by any individual. If consent is withdrawn, images are deleted, unless they form part of a record we are required to retain for legal or safeguarding reasons.

10. How we protect your information

- Clinical and business records are held in Google Workspace, accessed over encrypted connections
- Multi-factor authentication is enabled on all accounts with access to personal data
- Devices used to access records are encrypted at rest and protected by a password or biometric lock
- Where a therapist uses their own phone for work, the Thrive account on it is centrally managed, so that it can be required to have a screen lock and can be removed remotely if the device is lost or the therapist leaves
- Access is restricted to the therapists directly involved in a person's care, and to the Director
- Associates are granted access only to the records of the clients assigned to them, and that access is removed when the assignment or contract ends
- Paper records, where they are created in the course of a visit, are transported securely, transferred to the electronic record promptly, and then destroyed by cross-cut shredding
- Records are backed up in encrypted cloud storage
- Employees and associates complete data protection and safeguarding training at induction and annually thereafter
- We maintain a record of processing activities, a retention schedule, and a log of any data breaches

11. Children's and young people's information

For children, information is collected with the consent of a parent or a person with parental responsibility.

A young person aged 12 or over who has sufficient understanding of what is being asked may exercise their own data protection rights, including the right to see their own records. We assess this individually. From age 16 we presume a young person can give their own consent to treatment and exercise their own rights, unless there is reason to think otherwise.

Where a young person is competent to exercise their own rights, we will not disclose their records to a parent without their agreement, except where safeguarding requires it.

Children's information is used only for physiotherapy care, education and health provision, and medico-legal reporting where instructed. It is never used for marketing.

12. Self-employed associates

Associates working under the Thrive Physiotherapy name are required to sign a subcontractor agreement that includes data protection obligations, hold current HCPC registration and appropriate professional indemnity insurance, hold an Enhanced DBS certificate, complete data protection and safeguarding training, access only the client records necessary for their work, and return or securely delete all data when the relationship ends.

Where an associate is engaged to deliver care under our clinical governance, they act under our instruction in relation to personal data. Where an associate acts as an independent practitioner in their own right, that is made clear to the client in writing before the first appointment.

13. Your rights

You have the right to:

- **Be informed** about how we use your data, which is the purpose of this policy
- **Access** your data, by making a subject access request. We respond within one month. Where a request is complex we may extend this by up to two further months and will tell you if we do. There is no charge.
- **Rectification** of information that is inaccurate or incomplete
- **Erasure** of your data, where we have no continuing lawful reason to hold it. This right is limited for clinical records, which we are required to retain for the periods set out above.
- **Restrict processing** while a concern about accuracy or lawfulness is resolved
- **Data portability**, where processing is based on consent or contract and carried out by automated means
- **Object to processing** that we carry out on the basis of legitimate interests
- **Withdraw consent** at any time, where consent is the basis we rely on

To exercise any of these rights, email hello@thrivephysiotherapy.org.uk. We may ask you to confirm your identity before we release information.

Access to health records is subject to limited exemptions in Schedule 3 of the Data Protection Act 2018. We may withhold part of a record where releasing it would be likely to cause serious harm to the physical or mental health of any person, or where it contains information about another person who has not consented to its release. If we withhold anything we will tell you that we have done so and why, so far as we are able.

For the records of someone who has died, access is governed by the Access to Health Records Act 1990 rather than data protection law, and is available to a personal representative or to a person with a claim arising from the death.

14. Data breaches

If personal data is lost, disclosed in error, or accessed without authority, we will contain the incident, assess the risk to the people affected, and record it in our breach log.

Where a breach is likely to result in a risk to people's rights and freedoms we report it to the Information Commissioner's Office within 72 hours of becoming aware of it. Where the risk is high we also tell the people affected directly and without undue delay, and explain what has happened and what they can do.

15. Complaints

If you are unhappy with how we have handled your information, please tell us first, by email to hello@thrivephysiotherapy.org.uk. We will acknowledge your complaint within 5 working days and respond substantively within 20 working days.

You also have the right to complain to the Information Commissioner's Office at any time, whether or not you have raised the matter with us. The ICO can be reached at ico.org.uk/make-a-complaint or on 0303 123 1113.

16. Changes to this policy

We review this policy each August, and at any other time when we change a system, a supplier or a service that affects how personal data is handled. The version number and date at the top of this document show when it was last revised. Material changes are notified to current clients.