



1. Purpose

This Privacy Policy (Privacy Notice) explains how Kensington Square Therapy Ltd ("KST") collects, uses, stores, shares, and protects personal data in the course of delivering therapy, counselling, and wellbeing services to children, young people, families, and schools.

This notice fulfils KST's transparency obligations under Articles 13 and 14 of the UK General Data Protection Regulation (UK GDPR) and informs data subjects of their rights under UK data protection law.

2. Scope

This policy applies to all personal data processed by KST, across all settings:

- Private practice (Dyslexia Teaching Centre, 23 Kensington Square, London W8 5HN).
- School-based counselling and therapy provision within independent schools.
- Group programmes and facilitator-led services.

- Online and remote therapy delivered via encrypted video platforms.
- Administrative and business operations (invoicing, scheduling, compliance).

It applies to data relating to children and young people, parents and carers, school staff, referrers, subcontracted therapists and facilitators, website visitors, and enquirers.

This notice should be read alongside the KST Data Protection Policy, Cookie Policy, Safeguarding Policy, and Consent Form.

3. Definitions

- **Personal Data:** Any information relating to an identified or identifiable living individual, as defined by Article 4(1) UK GDPR.
- **Special Category Data:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, or data concerning a person's sex life or sexual orientation (Article 9 UK GDPR). Therapy notes and clinical records routinely contain health-related special category data.
- **Data Controller:** KST is the data controller for all personal data processed in connection with its services. This means KST determines the purposes and means of processing.
- **Data Processor:** A third party that processes personal data on behalf of KST (e.g. Konfidens, Google LLC).
- **Data Subject:** The individual to whom the personal data relates.
- **Processing:** Any operation performed on personal data, including collection, recording, storage, retrieval, use, disclosure, erasure, and destruction.
- **Gillick Competence:** The legal principle recognising that children under 16 who demonstrate sufficient understanding and intelligence may consent to or refuse medical treatment (and, by extension, therapy) independently of their parents.
- **DSAR:** Data Subject Access Request, a request by a data subject to obtain a copy of their personal data under Article 15 UK GDPR.

4. Legal and Regulatory Framework

This policy operates within the following legal and statutory framework:

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.

- Privacy and Electronic Communications Regulations 2003 (PECR).
- Children Act 1989 and Children Act 2004.
- Working Together to Safeguard Children 2023.
- Keeping Children Safe in Education 2024 (DfE).
- BACP Ethical Framework for the Counselling Professions.
- NCPS Code of Ethics.
- ICO Guidance on Children's Data and the Children's Code (Age Appropriate Design Code).
- Limitation Act 1980 (for retention periods).
- Finance Act 1998 / HMRC requirements (for financial records).

5. Data Controller and Contact Details

DATA CONTROLLER	
Company Name	Kensington Square Therapy Ltd
Company Number	16707111
ICO Registration	ZC022097
Registered Office	Flat 408, 2 Macfarlane Place, London W12 7RS (statutory filings only)
Trading Address	23 Kensington Square, London W8 5HN (Dyslexia Teaching Centre)
Data Protection Lead	Sam McManus (also Director and Designated Safeguarding Lead)
Contact Email	contact [at] kst.ltd
Finance Email	finance [at] kst.ltd
Website	www.kst.ltd
Insurer	Hiscox Underwriting Ltd, Policy OXY8749916
Subscriber-tier contact (The Parent Book)	hello [at] theparentbook.com
Subscriber-tier service	theparentbook.com/parents

KST is the independent data controller for all personal data processed in connection with its services. Where KST provides services within a school, KST and the school may operate as independent controllers in respect of their own records. KST does not act as a data processor for schools.

6. The Information We Collect

The personal data KST collects depends on the data subject's relationship with KST. KST collects only information that is necessary and relevant.

6.1 Children and Young People

- Name, date of birth, gender, school, and year group.
- Parent or guardian names and contact details.
- Relevant background information provided by parents, schools, or referrers to support therapy (e.g. educational, developmental, or family context).
- Session notes, assessments, and progress information (special category health data).
- Safeguarding records (where applicable).
- Attendance records.

6.2 Parents and Carers

- Name, contact details (email, telephone, address).
- Relevant family, educational, or contextual information shared in consultation or communication.
- Invoice and payment records (where applicable).
- Consent records.

6.3 Schools and Referrers

- School staff names, roles, and contact details.
- Referral information and presenting concerns.
- Progress summaries and safeguarding communications.
- Contractual and administrative information.

6.4 Subcontracted Therapists and Facilitators

- Name, contact details, qualifications, and professional body registrations.
- DBS certificate details, insurance documentation, and supervision records.
- Payment and invoicing records.
- Training and compliance records.

6.5 Website Visitors and Enquirers

- Information submitted through the website contact form (name, email, enquiry details).
- Cookie data and analytics data (see KST Cookie Policy).

- IP address and browser information collected via server logs.

Kensington Square Therapy uses Cloudflare Web Analytics, a privacy-first, cookieless analytics service, to understand aggregate visitor numbers and how the site is being used. Cloudflare does not store IP addresses, does not set cookies, and does not enable any individual visitor tracking. We do not use Google Analytics, advertising trackers, or any service that profiles you.

6.6 Individual Subscribers (The Parent Book)

Where you take out an individual subscription to The Parent Book at theparentbook.com/parents, KST collects:

- **Your subscriber email address.** The account is keyed to this address. It is used to sign you in by magic link, to email you about renewals, and to reach you about the subscription.
- **Your name, if you choose to give it.** Name is optional. If you do not give a name, we address you by the first part of your email address in renewal reminders.
- **Payment identifiers.** Bank details are held by GoCardless Ltd under the UK Direct Debit Scheme. KST does not see or store your bank details; it stores only the GoCardless customer, mandate and subscription IDs that link your account to your subscription.
- **Reading activity.** Which editions and articles you have opened, and when. Used for in-house product analytics only. Not used for advertising, not sold, and not shared with any third-party analytics service.
- **Operational metadata.** Magic-link and sign-in timestamps, device user-agent strings for session security, and IP address kept in server logs for 30 days then rotated. No precise location tracking.
- **Consent records.** The state and timestamp of your immediate-access waiver at checkout and your marketing-email opt-in if given, kept to evidence the lawful basis under Article 7(1) UK GDPR.
- **Family personalisation details, if you choose to give them.** To have the library lead with what fits your family, you can tell us each child's age or year group and their school. This is optional, the library works without it, and you can change or delete it at any time from your account page. We store only the age or year group and the school, never the child's name and nothing clinical. We use it only to default your library view to the pieces most relevant to your family and to time the school-year letters. It is held on your own subscriber record, and it is never shared.

What KST does not collect about subscribers. KST does not collect or process special category data about subscribers in connection with the subscription. KST does not intentionally collect any personal data about a subscriber's child or other family member through the subscription, beyond the optional family personalisation details described above (a child's age or year group and school, never a name and nothing clinical), which you provide and can remove at any time.

7. Lawful Bases for Processing

KST processes personal data under the following lawful bases as defined by Article 6(1) UK GDPR:

PROCESSING ACTIVITY	LAWFUL BASIS (ART. 6)	EXPLANATION
Delivering therapy and counselling	Contract (Art. 6(1)(b))	Necessary for performance of the therapy service agreement with the client or their parent/carer.
Safeguarding and child protection	Legal obligation (Art. 6(1)(c)); Vital interests (Art. 6(1)(d))	Required by Children Act 1989/2004, Working Together 2023, and KCSIE 2024.
Clinical record keeping	Legal obligation (Art. 6(1)(c)); Legitimate interests (Art. 6(1)(f))	Professional and regulatory requirement; legitimate interest in defensible clinical practice.
School reporting and communication	Legitimate interests (Art. 6(1)(f))	Necessary for effective school-based provision; balanced against data subject rights.
Parent communication and updates	Contract (Art. 6(1)(b)); Consent (Art. 6(1)(a))	Contractual where part of service agreement; consent-based for discretionary sharing.
Financial administration	Legal obligation (Art. 6(1)(c))	HMRC accounting and tax obligations.
Supervision (clinical)	Legitimate interests (Art. 6(1)(f))	Professional requirement; names typically anonymised.
Website contact form enquiries	Legitimate interests (Art. 6(1)(f))	Responding to enquiries from prospective clients.
Website analytics (aggregate, cookieless)	Consent (Art. 6(1)(a))	Cloudflare Web Analytics sets no cookies and stores no IP addresses. Event beacons on pages carrying the consent banner fire only when the Analytics option is enabled (see Cookie Policy).
Delivering The Parent Book individual subscription (access, magic-link sign-in, renewal reminders)	Contract (Art. 6(1)(b))	Necessary for performance of the subscription contract.
Taking subscription payments and reconciling them	Contract (Art. 6(1)(b)); Legal obligation (Art. 6(1)(c))	Necessary for the contract and for HMRC and Companies Act 2006 record-keeping.
Subscriber product analytics (reading activity, in-house only)	Legitimate interests (Art. 6(1)(f))	Understanding which editions serve subscribers; balanced by in-house-only processing, no third-party analytics, no advertising profiling, and 12-month anonymisation. Subscribers may object.
Storing optional family personalisation details (a child's age or year group and school) to tailor the library and time the school-year letters	Consent (Art. 6(1)(a))	Given by ticking the personalisation consent box on the account page; editable or deletable there at any time; withdrawal is effective immediately and does not affect the subscription.
Service emails and account security (renewal reminders, magic-link emails, sign-in metadata)	Contract (Art. 6(1)(b)); Legitimate interests (Art. 6(1)(f))	Necessary to deliver and secure the subscription. Not marketing communications.
Marketing emails about new editions and resources	Consent (Art. 6(1)(a)); PECR 2003 reg 22	Separate, unticked-by-default opt-in at signup, toggleable on the account page. One-click unsubscribe; withdrawal is immediate and does not affect the subscription.

7.1 Special Category Data (Article 9)

Therapy notes, clinical assessments, and safeguarding records contain health-related special category data. KST processes this data under the following conditions:

- **Article 9(2)(a):** Explicit consent, obtained through the KST Consent Form at the start of therapy.

- **Article 9(2)(b):** Employment, social security, and social protection obligations, where processing is necessary for safeguarding purposes.
- **Article 9(2)(c):** Vital interests, where necessary to protect the life of the data subject or another person, and the data subject is incapable of giving consent.
- **Schedule 1, Part 1, Paragraph 2 DPA 2018:** Health or social care purposes.

7.2 Children's Data

KST processes the personal data of children and young people in accordance with the ICO's Children's Code (Age Appropriate Design Code) principles. Where a child is assessed as Gillick competent, KST will seek the child's own views regarding data sharing, particularly in relation to progress updates to parents and schools.

KST does not profile children, make automated decisions about children, or use children's data for marketing purposes.

The Parent Book individual subscriber tier is a service for adult parents and carers. Where a subscriber chooses to personalise their library, KST stores a child's age or year group and their school on the parent's account, with the parent's consent, to shape which chapters lead and to time the school-year letters. KST does not collect the child's name, does not link reading activity to any individual child, holds no clinical or special category data about a child through the subscription, and does not profile any child. The ICO's Children's Code is engaged for KST's clinical services to children (Sections 6.1 and 7.2) but is not engaged for the subscriber tier, which has no child user and holds no identifying child data.

8. Sharing Information

KST respects confidentiality and shares personal data only when necessary, lawful, and proportionate. KST will aim to discuss any necessary sharing with the data subject (or their parent/carer) in advance, unless doing so would increase risk to a child or vulnerable person.

KST may share limited personal data with the following recipients:

- **Clinical supervisors:** To support ethical and effective practice. Names are anonymised unless the nature of the concern requires identification.
- **Schools:** Where a child is seen as part of a school counselling programme. Sharing is limited to what is necessary for the child's welfare and the school's safeguarding duties.
- **Parents and carers:** Progress updates are provided with the child's agreement (where the child is Gillick competent). Detailed session content is not routinely shared.
- **Safeguarding agencies:** Local authority children's services, police, or the Local Authority Designated Officer (LADO) where there is a serious safeguarding concern. This may occur without the data subject's consent where necessary to protect a child.
- **Accountants and regulators:** For lawful compliance (financial records only).

- **Insurers:** In the event of a claim or regulatory enquiry (limited to what is necessary).

KST does not sell, rent, or trade personal data. KST does not share personal data for marketing purposes.

8.1 Sub-processors (The Parent Book subscriber tier)

KST uses the following sub-processors to operate the individual subscriber tier. Each acts as a processor under UK GDPR, processes personal data only on KST's documented instructions, and is bound by a written agreement consistent with Article 28 UK GDPR.

SUB-PROCESSOR	PURPOSE AND DATA	LOCATION AND TRANSFER
GoCardless Ltd (UK, FCA FRN 597190)	Direct debit mandate setup and recurring payment collection. Subscriber name (optional), email, bank account details, GoCardless IDs.	UK. No international transfer engaged.
Cloudflare, Inc.	Site hosting, edge delivery and KV storage for subscriber records. Subscriber email, account state, reading activity, transient IP in edge logs.	UK/EU region for KV storage. UK IDTA and EU SCCs for any onward transfer.
Resend Inc.	Transactional email delivery (magic-link, renewal, welcome and account emails). Subscriber email and email content.	Resend EU region (eu-west-1, Ireland). No onward international transfer engaged.
Google LLC	Google Workspace for administrative and financial records, including subscriber correspondence. Subscriber email, correspondence, invoice records.	US, with UK/EU residency where supported. UK IDTA; Workspace UK Addendum.
Xero	Accounting records for subscription income. Subscriber email, invoice metadata, payment amounts.	UK, EU and Australia. UK IDTA and EU SCCs per Xero DPA.

KST does not use third-party advertising networks, third-party analytics platforms, customer data platforms, or marketing-automation platforms for the subscriber tier, other than the optional marketing-email opt-in, which uses Resend only. KST does not sell, rent or trade subscriber personal data, and does not share it for marketing purposes.

9. Data Storage and Security

KST uses secure, encrypted systems to store and manage personal data:

DATA STORAGE SYSTEMS	
Clinical records (therapy notes)	Konfidens, operated by Mindcare AS (trading as Konfidens); a GDPR-compliant, encrypted clinical records platform, data encrypted in transit and at rest and hosted within the EEA (AWS, Frankfurt, Germany)
Administrative records	

Google Workspace (Drive, Gmail, Sheets, Forms), encrypted, access-controlled

Financial records

Google Workspace and Xero (where applicable)

Website contact form submissions

Fluent Forms via WordPress, server-hosted, access-controlled

Paper records

Locked cabinet at trading address; destroyed by cross-cut shredding when no longer required

Security measures include:

- All devices are password-protected, encrypted, and subject to automatic screen lock.
- Multi-factor authentication (MFA) is enabled on all KST accounts.
- Access to clinical records is restricted to the assigned therapist and the Director.
- No personal data is stored on personal devices or unencrypted removable media.
- Regular review of access permissions and account security.

Subscriber records for The Parent Book (email, name where given, GoCardless identifiers, reading activity, optional family personalisation details, account state) are stored in Cloudflare KV in the UK/EU region, encrypted at rest and in transit. Access is restricted to the Director and to deployment automation. Subscriber correspondence and accounting records sit in Google Workspace and Xero as set out above.

9.1 Cookies on the subscriber tier

The Parent Book /parents pages use one first-party, strictly necessary cookie, `tpb_sess`, which keeps you signed in after you click a magic link (HttpOnly; Secure; SameSite=Lax; expires 90 days from last sign-in). Its lawful basis is the PECR 2003 reg 6(4)(b) strictly-necessary exemption. No analytics, advertising or third-party cookies are set on the subscriber tier, and it embeds no third-party scripts, pixels or trackers.

9.2 Konfidens sub-processors (clinical records)

Clinical records are held in Konfidens, operated by Mindcare AS (org. no. 925 239 070), Oslo, Norway. Konfidens acts as KST's processor under a written data processing agreement (Article 28 UK GDPR) and engages the sub-processors below, which may process personal data, including special category health data, that KST enters into the platform. The current authoritative list is maintained by Konfidens at konfidens.com/sub-processors.

SUB-PROCESSOR	LEGAL ENTITY	PURPOSE	PROCESSING LOCATION	
Amazon Web Services	Amazon Web Services EMEA SARL (Luxembourg)	Hosting, database and file storage for the platform	Frankfurt, Germany (eu-central-1)	
Microsoft Azure	Microsoft Ireland Operations Limited	AI Scribe text processing and session summarisation (text transcripts only, no audio, deleted within 48 hours)	Norway	
Speechmatics	Speechmatics Ltd (United Kingdom)	AI Scribe speech-to-text (transcribed in real time, no audio stored)	United Kingdom	
Whereby	Whereby AS (Norway)	Secure video consultations (no recordings stored)	EU/EEA	
Adyen	Adyen N.V. (Netherlands)	Processing of patient payments to the practitioner, and refunds	Europe	
GatewayAPI	GatewayAPI A/S (Denmark)	SMS for authentication and appointment reminders	Germany, Finland, Denmark	
Brevo	Brevo SAS (France)	Transactional email from the platform (no health information sent by email)	Germany, Belgium, Ireland	
Criipto	Criipto ApS (Denmark)	BankID identification and authentication (Norwegian users only)	Norway	
hCaptcha	Intuition Machines, Inc. (United States)	Bot detection and fraud prevention on login and registration	Primarily EU; limited log metadata may be processed in the United States (see Section 10)	

Konfidens notifies KST at least 14 days before adding or replacing a clinical-records sub-processor, giving KST an opportunity to object. Not all of these sub-processors are engaged for every practice; those tied to features KST does not use (for example the AI Scribe or BankID) do not process KST data unless and until that feature is used.

10. International Data Transfers

Google Workspace data may be processed on servers located outside the United Kingdom. Google LLC operates under UK International Data Transfer Agreement (IDTA) safeguards and has certified compliance with applicable data protection standards.

Konfidens (Mindcare AS) hosts clinical data within the EEA, on Amazon Web Services in Frankfurt, Germany, encrypted in transit and at rest. Konfidens and its sub-processors process within the EEA and the United Kingdom; transfers between the two rely on the UK and EU adequacy decisions. Where a Konfidens sub-processor processes limited data in the United States (currently hCaptcha, for bot detection at login and registration), that transfer relies on the provider's EU-US and UK-US Data Privacy Framework certification, supported by the EU Standard Contractual Clauses and the UK International Data Transfer Addendum.

KST reviews the transfer mechanisms of its data processors annually and will update this notice if the legal basis for international transfers changes.

For The Parent Book subscriber tier, the principal international-transfer considerations are Google Workspace (US) and Xero (UK, EU and Australia), both under the UK IDTA supplemented by each provider's data processing agreement. Resend is EU-hosted (eu-west-1) and does not engage an onward international transfer.

GoCardless and Cloudflare KV storage are UK/EU.

11. How Long We Keep Information

KST retains personal data only for as long as necessary. The following retention periods apply:

RECORD TYPE	RETENTION PERIOD	LEGAL BASIS
Therapy notes (child clients)	Seven years after end of therapy, or until the child reaches age 25, whichever is longer	Limitation Act 1980; professional guidance
Therapy notes (adult clients)	Seven years after end of therapy	Limitation Act 1980
Safeguarding records	Retained in line with local authority guidance; may exceed standard retention	Children Act 1989; Working Together 2023
Consent forms	Duration of therapy plus seven years	Contractual and legal obligation
Invoices and financial records	Six years from end of financial year	HMRC requirements; Finance Act
Subcontractor records (DBS, insurance)	Duration of engagement plus six years	Legal obligation; insurance requirements
Website contact form submissions	Twelve months, or until enquiry resolved	Legitimate interests
Complaints records	Six years from date of closure	Limitation Act 1980
DSAR records	Three years from date of response	ICO accountability requirements
Subscriber account records (email, name, GoCardless IDs, subscription status)	While active, and six years after final payment	Companies Act 2006; HMRC; Limitation Act 1980
Subscriber reading activity (identifiable)	Twelve months, then anonymised	Legitimate interests (product analytics)
Optional family personalisation details (child's age or year group, school)	While stored on the account; deleted on removal or when the subscription ends	Consent (Art. 6(1)(a)); minimum-necessary
Subscriber IP address logs	30 days, then rotated	Legitimate interests (security)
Subscriber consent records (waiver, marketing opt-in)	While relied upon, and six years after withdrawal or end of subscription	Article 7(1) UK GDPR; Limitation Act 1980

After the applicable retention period, records are securely deleted (electronic) or destroyed by cross-cut shredding (paper). Deletion is logged.

12. Your Data Rights

Under UK GDPR, data subjects have the following rights:

- **Right of access (Article 15):** To obtain a copy of your personal data held by KST.
- **Right to rectification (Article 16):** To request correction of inaccurate personal data.
- **Right to erasure (Article 17):** To request deletion of personal data where there is no compelling reason for continued processing. This right is subject to exceptions, including legal obligations and safeguarding duties.
- **Right to restriction (Article 18):** To request that processing is restricted in certain circumstances (e.g. while accuracy is contested).
- **Right to data portability (Article 20):** To receive personal data in a structured, commonly used format and to transmit it to another controller.
- **Right to object (Article 21):** To object to processing based on legitimate interests. KST will cease processing unless there are compelling legitimate grounds.
- **Rights relating to automated decision-making (Article 22):** KST does not carry out automated decision-making or profiling.

To exercise any of these rights, contact the Data Protection Lead at contact [at] kst.ltd. KST will respond within one calendar month. Identity verification may be required before information is released. Complex or numerous requests may be extended by a further two months, with notification provided within the first month.

Where a request is made by a parent on behalf of a child who is assessed as Gillick competent, KST will consider the child's own views before responding.

12.1 Exercising your rights as an individual subscriber

If you hold a Parent Book subscription, you can exercise any of the rights above by emailing hello [at] theparentbook.com from your subscriber email address. In particular, you may withdraw the optional family personalisation at any time by editing or deleting it on your account page, or by asking us; you may object to reading-activity analytics, after which KST stops linking reading activity to your account and anonymises the historical record; and you may withdraw marketing consent at any time with no effect on your subscription. Where KST must retain a limited financial record for six years under the Companies Act 2006 and HMRC rules, it will explain what has been kept and why.

13. Safeguarding and Legal Exceptions

Confidentiality is central to effective therapy but cannot be absolute. KST may share limited personal data without the data subject's consent where:

- A child or young person is at risk of significant harm or abuse.
- An adult is at risk of serious harm.
- There is a risk to the welfare of a child as defined by Working Together to Safeguard Children 2023.
- Disclosure is required by law (e.g. a court order, statutory enquiry, or police investigation).
- Disclosure is necessary to prevent a serious crime.

Any such sharing is proportionate, recorded, and reported to the Director (as DSL). For full details, see the KST Safeguarding Policy.

14. If Therapy Ends or You Change Schools

When therapy concludes, records are securely stored for the applicable retention period set out in Section 11.

If a child changes school or moves to another therapist, KST can provide a brief handover summary to the new provider with written consent from the parent (and the young person's consent, where the child is Gillick competent). Records are never transferred automatically.

At the end of the retention period, records are securely deleted or destroyed. KST encourages discussion about record management at the conclusion of therapy.

15. Data Breach Response

In the event of a personal data breach, KST will follow the KST Data Breach Response Plan (v1.0-2026). Where a breach poses a risk to the rights and freedoms of individuals, KST will notify the Information Commissioner's Office within 72 hours and, where the risk is high, will notify affected individuals without undue delay.

16. Risk Management

RISK	MITIGATION	LIKELIHOOD	IMPACT
Unauthorised access to clinical records	Konfidens access controls; MFA; device encryption; annual access review	LOW	HIGH
Data shared without lawful basis	Lawful basis documented per processing activity; consent forms; staff training	LOW	HIGH
Retention periods not enforced	Retention schedule maintained; annual deletion review; deletion logged	MEDIUM	MEDIUM
DSAR not responded to within statutory timeframe	DSAR procedure documented; response template maintained; Director tracks deadlines	LOW	MEDIUM
International transfer safeguards change	Annual review of processor transfer mechanisms; IDTA monitoring	LOW	MEDIUM
Child's Gillick competence not assessed before sharing	Gillick assessment documented; therapist training; consent form addresses this	LOW	HIGH
Data breach not detected or reported	Breach response plan; incident reporting training; Konfidens audit logs; Google Workspace audit	LOW	HIGH

17. Record Keeping

- **Record of Processing Activities (ROPA):** Maintained by the Data Protection Lead, documenting all processing activities, lawful bases, recipients, transfers, and retention periods.
- **Consent Records:** Signed consent forms stored securely in Google Workspace.
- **DSAR Log:** All data subject access requests recorded and tracked.
- **Breach Register:** All personal data breaches logged, regardless of whether ICO notification was required.
- **Data Processor Register:** Register of all third-party processors with DPA status and review dates.

All records are stored securely within Google Workspace with access restricted to the Director.

18. Training Requirements

- **Director / Data Protection Lead:** UK GDPR compliance, DSAR handling, breach response, children's data, ICO guidance updates. Reviewed annually.
- **Subcontracted Therapists and Facilitators:** Data protection awareness, confidentiality boundaries, safeguarding interface, secure record keeping. Covered at induction and reviewed annually.

Training completion is recorded in the KST Training Log.

19. Monitoring and Audit

- **Annual data protection audit:** Review of all processing activities, lawful bases, retention compliance, processor agreements, and security measures.
- **ROPA review:** Record of Processing Activities updated at least annually.
- **Processor review:** Annual review of all data processor agreements and international transfer mechanisms.
- **ICO guidance monitoring:** Data Protection Lead monitors ICO publications, enforcement actions, and guidance updates.

20. How to Contact Us or the ICO

If you have any questions or concerns about how KST handles your personal data, please contact:

KST DATA PROTECTION LEAD	
Name	Sam McManus
Email	contact [at] kst.ltd
Address	Kensington Square Therapy Ltd, 23 Kensington Square, London W8 5HN

If you are dissatisfied with how your data has been handled, you have the right to lodge a complaint with the Information Commissioner's Office:

INFORMATION COMMISSIONER'S OFFICE

Website ico.org.uk/make-a-complaint

Helpline 0303 123 1113

KST recommends raising any concern with the Data Protection Lead in the first instance, as many issues can be resolved directly and promptly.

20.1 Complaints from individual subscribers

Complaints about the individual subscriber tier follow The Parent Book complaints procedure: email hello [at] theparentbook.com with the heading "Complaint". KST acknowledges within five working days and responds substantively within 20 working days. You may complain to the Information Commissioner's Office at any time using the details above.

21. Review Cycle

This policy will be reviewed annually or sooner if:

- UK GDPR, DPA 2018, or ICO guidance changes.
- A data breach, DSAR, or complaint identifies a need for revision.
- KST introduces new processing activities, systems, or service settings.
- A data processor changes its terms or transfer mechanisms.
- The annual data protection audit identifies weaknesses.

22. Related Policies

- KST Data Protection Policy (v1.0-2025)
- KST Cookie Policy (v1.0-2026)
- KST Terms of Use (v1.0-2026)
- KST Safeguarding Policy
- KST Confidentiality Policy
- KST Consent Form (v1.0-2026)
- KST Data Breach Response Plan (v1.0-2026)
- KST DSAR Procedure (v1.0-2026)

- KST Complaints Procedure (v1.0-2026)
- The Parent Book Terms of Subscription (v2.0-2026)
- The Parent Book Refund Policy (v2.0-2026)
- The Parent Book Privacy Notice (theparentbook.com/privacy)

23. Governance Maturity Assessment

GOVERNANCE MATURITY	
Current Maturity Level	Level 4 – Audit Ready
Target Maturity Level	Level 5 – Board-Level Best Practice
Actions to Reach Target	Complete ROPA; implement automated retention enforcement; conduct tabletop DSAR exercise; integrate privacy impact assessments into service design
12-Month Target	Achieve Level 5 through documented ROPA, evidenced annual audit, tabletop exercises, and privacy-by-design integration

24. Version Control

VERSION	AUTHOR	APPROVED BY	DATE ISSUED	REVIEW DATE	SUMMARY OF CHANGES
1.0	Sam McManus	Sam McManus	October 2025	October 2026	Initial release
2.0	Sam McManus	Sam McManus	February 2026	February 2027	Major revision: restructured to 24-section governance format; lawful basis table added; retention schedule table added; international transfers section added; children's data and Gillick competence addressed; risk register added; DPIA position stated; governance maturity assessment added
3.0	Sam McManus	Sam McManus	August 2026	August 2027	Added The Parent Book individual subscriber tier: new data subject category 6.6 (Individual Subscribers) including optional family personalisation (a child's age or year group and school, held with consent, minimised, never the child's name and nothing clinical, deletable at any time, never shared); children's-data note extended for the subscriber tier; lawful bases for subscription processing including personalisation on Art. 6(1)(a) consent and marketing email under PECR 2003 reg 22; sub-processor table (GoCardless, Cloudflare, Resend, Google, Xero); subscriber storage, international transfers and retention; subscriber-tier cookie (tpb_sess); subscriber rights and complaints routes. Aligned with The Parent Book Privacy Notice. Company number 16707111 and registered and trading addresses confirmed.
3.1	Sam McManus	Sam McManus	September 2026	August 2027	Clinical records processor updated from Kiku to Konfidens, operated by Mindcare AS (trading as Konfidens), under an Article 28 data processing agreement; clinical data encrypted in transit and at rest and hosted within the EEA on AWS in Frankfurt, Germany. Added the itemised Konfidens clinical-records sub-processor list (Section 9.2) and updated the definitions, storage, international-transfers and risk sections accordingly.