Data Protection Policy

Version 3.2 | June 2026 | Next Review date: June 2027
Approved by: Jackie Lindeck, Rachael Aylmer and Gabrielle Stirling - Company Directors

This policy is part of a suite of documents

- Data Protection Policy (this document): the authoritative policy on how PP handles personal data
- Data Protection Plain-English Summary: an accessible guide for families, practitioners and associates
- AI Use Policy (separate document): governing the use of AI tools in PP's work
- Recording Consent Form (separate document): to be completed before any session is recorded
- Privacy and Cookies Policy: view online here
- Associate Contract: which incorporates a Data Processing Agreement at Section 9

All documents are available from the Data Protection Officer:
gabrielle@partnershipprojectsuk.com

1. Introduction

This Policy sets out the obligations of PartnershipProjects UK Ltd ("PP" or "the Company") regarding data protection and the rights of clients, families, professionals, and business contacts ("data subjects") under the Data Protection Act 2018 and the UK General Data Protection Regulation ("UK GDPR").

It applies to all employees, associates, contractors, volunteers, and trainees working on behalf of PP. Compliance is mandatory. PP is committed not only to the letter of the law, but to the spirit of it, handling all personal data with care, transparency, and respect.

Data Protection Officer: Gabrielle Stirling | gabrielle@partnershipprojectsuk.com | +44 (0) 330 808 0644

IT Administrator: Rose McGowan | rose@partnershipprojectsuk.com

2. Key definitions

Term	Meaning
Personal data	Any information relating to an identifiable living person
Special category data	Personal data requiring extra protection which includes health data, mental health information, and family welfare information. All therapeutic session content falls into this category.
Data controller	The organisation that determines why and how personal data is processed. PP is the data controller.

Term	Meaning
Data processor	A person or organisation that processes data on behalf of the controller. Associates and contractors acting for PP are data processors.
UK GDPR	The UK General Data Protection Regulation; the primary data protection law in the UK following Brexit.
ICO	The Information Commissioner's Office; the UK's data protection regulator.

3. The data protection principles

All personal data processed by PP and those working on its behalf must be:

- Processed lawfully, fairly, and transparently
- Collected for specified, explicit, and legitimate purposes only
- Adequate, relevant, and limited to what is necessary
- Accurate and kept up to date
- Kept no longer than necessary
- Kept secure against unauthorised access, loss, or damage

4. Lawful basis for processing

PP must have a lawful basis for processing any personal data. For general personal data, the lawful basis will typically be one of: consent; performance of a contract; legal obligation; protection of vital interests; or legitimate interests.

Because therapy session content is special category data (health data), a further condition must also be met. PP relies primarily on explicit consent for processing special category data, supplemented where necessary by the basis of legal claims or vital interests.

Where consent is the basis for processing, it must be freely given, specific, informed, unambiguous, and documented. Data subjects may withdraw consent at any time.

5. Data controller and processor responsibilities

PP acts as the data controller for all personal data processed in the course of its business and therapeutic services.

Associates and self-employed contractors who process client data on PP's behalf are data processors. UK GDPR Article 28 requires a written Data Processing Agreement (DPA) to govern this relationship. This is incorporated into the associate contract at Section 9. No associate or contractor may process client data on PP's behalf without a signed contract in place.

Associates and contractors must:

- Process client data only in accordance with PP's instructions
- Implement appropriate security measures
- Not engage any sub-processor without PP's written approval
- Report any actual or suspected data breach to PP without delay
- Return or securely delete all personal data upon termination of their engagement

6. Personal data collected and processed

PP collects and processes the following categories of personal data:

- Contact information: name, phone number, email address

- Professional information: qualifications, professional registration details (staff and associates)
- Therapeutic and clinical information: session notes, assessment summaries, care plans, and professional correspondence; special category data
- Family and child information: details relevant to therapeutic work; special category data
- Safeguarding information: where required for the protection of children or vulnerable adults; special category data
- Financial information: invoicing and payment records

Data is only collected to the extent necessary for the specific purpose for which it is needed. Data subjects are informed of the purpose at the point of collection.

7. Data retention

PP retains personal data only for as long as is necessary. The following schedule applies:

Record type	Retention period	Basis
Therapy session notes: adults	7 years from end of therapy	Limitation Act 1980; ICO; HCPC/BACP/UKCP
Therapy session notes: children	Until the child's 25th birthday (or 7 years if longer)	NHS Records Code; ICO; child safeguarding best practice
Assessments, care plans, correspondence	As above (adult or child schedule)	As above
Session recordings (where made)	30 days default; 90 days maximum	Data minimisation; UK GDPR; BACP/UKCP
AI-generated draft notes	Deleted within 24 hours of note completion	Data minimisation; UK GDPR Article 5
Consent forms	7 years (adults); until age 25 (children)	Evidence of lawful processing
Financial and invoicing records	7 years	HMRC requirements
Employee / associate records	7 years after end of engagement	Employment law; limitation periods
Data breach records	Minimum 5 years	ICO accountability requirements

When the retention period expires, records must be securely deleted (electronic) or shredded (paper). Disposal must be documented and the DPO notified.

Handwritten notes must be scanned and uploaded to the practitioner's designated Google Drive folder, and the paper originals then shredded. Both copies must not be retained simultaneously.

8. Data security

Storage

- Electronic records must be stored securely using passwords and encryption via PP Google Workspace. **see more information below.
- Paper records must be kept in a locked cabinet or equivalent
- No clinical data should be stored on personal devices, personal cloud storage, or personal email accounts

Interim clinical records storage arrangement

Session notes and clinical records are currently stored in individual, access-restricted folders within the organisation's Google Workspace shared drive. Each associate or practitioner has their own designated folder, accessible only to them, the Data Protection Officer and the IT Administrator.

The Google Workspace Data Processing Addendum is in place, and we have opted for our storage to be held within Europe. PP recognises that Google Workspace is not purpose-built for clinical records and is committed to moving to a dedicated clinical record keeping system as appropriate, affordable solutions become available.

In the meantime, all practitioners must store clinical records only in their designated PP Google Drive folder, follow the security and retention requirements set out in this policy, and must not store clinical records in any other location, including personal devices, personal cloud storage, or personal email accounts.

Google Workspace**

PP uses Google Workspace for organisational administration, communications, and interim clinical record storage. The following requirements apply to all staff and associates:

- The Google Workspace Data Processing Addendum must be accepted in the admin console (Account settings > Legal & compliance) the DPO is responsible for confirming this is in place
- All staff and associates must use PP's Workspace accounts only, not personal Gmail or Google accounts, for any PP-related activity
- Clinical records must be stored only in the practitioner's designated PP Google Drive folder, not in any shared or open folder
- Access to each practitioner's folder must be restricted to that practitioner, the DPO and IT Administrator only
- Google's AI features (including Gemini) must not be used in connection with any client-related content

Communications

- Personal data must only be transmitted over secure networks
- Emails containing personal data should be marked confidential and avoid including detailed clinical content in the body of the email where possible
- Personal data must not be sent via personal email accounts
- Hard copy personal data must be sent via Royal Mail Signed For or equivalent, in a sealed container marked confidential

IT security

- Passwords must be strong, changed regularly, and never shared
- 2-step-verification (2SV) is enforced across the organisation
- All software must be kept up to date with security patches applied promptly
- No software may be installed on PP-owned devices without prior approval

9. Online therapy and session recording

PP delivers therapy primarily via secure online video platforms. Appropriate security measures (password-protected meetings, waiting rooms, encryption) are used as standard.

Recording

Sessions are not recorded as standard practice. Recording will only take place where there is a clear and documented purpose, explicit written consent has been obtained using the PP Recording Consent Form, and the recording is stored securely and deleted at the end of the retention period.

See separate document

Recording Consent Form — must be completed separately from general therapy consent before any session is recorded.

Recordings must never be used for marketing, AI processing outside an approved workflow, or any secondary purpose without fresh consent. Families may decline recording at any time without this affecting their therapy.

AI tools and note generation

The use of AI tools is governed by PP's AI Use Policy. In summary:

- Only approved AI tools may be used; no tool may be introduced without DPO approval
- Separate, explicit written consent is required before any AI tool is used in connection with a session
- AI-generated outputs are working drafts only; the practitioner's written notes are the clinical record
- AI-generated recordings and transcripts must be deleted within 24 hours of the notes being completed
- Zoom's built-in AI Companion and equivalent platform AI features must not be used during therapy sessions

See separate document

AI Use Policy sets out the full requirements, approved tools, prohibited uses, and practitioner responsibilities.

10. Consent

Where PP relies on consent as the lawful basis for processing, consent must be freely given, specific, informed, unambiguous, and documented. Data subjects may withdraw consent at any time.

Consent for therapy, consent for recording, and consent for AI note-generation tools are three separate consents and must each be obtained individually.

11. The rights of data subjects

Under UK GDPR, data subjects have the following rights. All requests should be directed to the DPO and responded to within one month.

Right	What it means
To be informed	To know what data PP holds, why, and how it is used
Of access	To request a copy of personal data held (Subject Access Request)
To rectification	To have inaccurate or incomplete data corrected
To erasure	To request deletion of personal data in certain circumstances (note: legal and professional retention obligations may limit this right)

Right	What it means
To restrict processing	To request that PP stops actively processing data in certain circumstances
To data portability	To receive personal data in a structured, commonly used format
To object	To object to processing based on legitimate interests or for direct marketing

Subject Access Requests should be made in writing to the DPO. PP does not charge a fee for standard requests.

12. Keeping data subjects informed

Where personal data is collected directly from a data subject, they will be informed at the point of collection of: the identity and contact details of PP and the DPO; the purpose and lawful basis for processing; how long data will be retained; their rights; and their right to complain to the ICO.

Where personal data is obtained from a third party, the data subject will be informed within one month, or when first communicated with, whichever is earlier.

13. Transfers of data outside the UK

Personal data may only be transferred outside the UK where an adequacy regulation applies, appropriate safeguards are in place, the data subject has given informed consent, or the transfer is necessary for legal or vital interest purposes. Any third-party software or cloud platform processing data outside the UK must be reviewed by the DPO before use.

14. Data Protection Impact Assessments

A DPIA must be conducted before any new project, system, or tool involving personal data is introduced, including any new software, AI tool, or video platform. DPIAs are overseen by the DPO.

15. Data breaches

A data breach is any event where personal data is accessed, disclosed, lost, destroyed, or altered without authorisation.

1. **Report immediately.** Any actual or suspected breach must be reported to the DPO without delay. Do not investigate independently.
2. **ICO notification.** Where a breach is likely to result in a risk to data subjects' rights, the DPO must notify the ICO within 72 hours.
3. **Individual notification.** Where a breach poses a high risk, affected individuals must be informed directly without undue delay.

Breach records must be maintained by the DPO and retained for a minimum of five years.

16. Organisational responsibilities

PP will ensure that all staff, associates, and contractors are aware of their data protection responsibilities; that access to personal data is limited to those who need it; that everyone handling personal data is appropriately trained; and that data processing methods are

regularly reviewed. Associates and contractors are bound by equivalent obligations through their contracts.

The DPO is responsible for overseeing implementation of this Policy, maintaining records of processing activities, conducting DPIAs, and acting as the primary contact for data protection matters.

Policy title	Data Protection Policy
Version	3.2 (updated June 2026 — interim storage position)
Review date	June 2027
Approved by	Jackie Lindeck, Rachael Aylmer and Gabrielle Stirling - Company Directors
DPO	Gabrielle Stirling — gabrielle@partnershipprojectsuk.com
Related documents	AI Use Policy | Recording Consent Form | Plain-English Summary | Associate Contract (Section 9)

This document is the authoritative data protection