



Data Management Policy – March 2025

Phoenix Psychology Collective Ltd

Last updated: March 2025

1. Purpose and Scope

This policy outlines how Phoenix Psychology Collective Ltd (PPC) and its affiliated practitioners manage, store, and protect personal data in compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and relevant guidance from professional bodies (e.g. HCPC, BPS, AEP).

It applies to all staff, associates, and subcontracted practitioners who access or handle client data as part of delivering psychological services.

2. Our Commitment to Data Protection

Phoenix Psychology Collective is committed to:

- Upholding the privacy and confidentiality of all client data
- Ensuring secure storage and transmission of personal information
- Responding promptly to data breaches and information requests
- Supporting all practitioners to act as responsible data handlers

3. Roles and Responsibilities

- **Phoenix Psychology Collective Ltd** acts as the Data Controller for all organisational data processes and oversees GDPR compliance across the service.
- All practitioners are responsible for:
 - Registering as **Data Controllers** with the ICO (if operating as sole traders)
 - Conducting regular **data audits**

- Following PPC policies and the data protection guidance of their professional bodies

4. Data Collection and Use

PPC collects and processes personal and special category data (e.g. health, education, social/emotional information) only for the purpose of providing psychological services to children, young people, and their families.

Practitioners must ensure:

- Only relevant information is collected
- Clients (or those with parental responsibility) give **informed consent** for assessment, intervention, and any data sharing

5. Data Storage and Security

Electronic Data

- All client data must be stored using **secure, encrypted cloud platforms** (e.g. Microsoft OneDrive)
- Devices used to access data must be:
 - Password or PIN protected
 - Logged out of cloud/email systems when unattended
 - Configured with remote-wipe functionality if possible
- Practitioners must ensure:
 - **Shared or personal devices** used for work are secured
 - Others (e.g. family members, repair technicians) cannot access client information

Paper Records

- Paper records must be:
 - Kept to a minimum
 - Stored in locked filing cabinets or safes
 - Never left unattended or visible in shared spaces
- Printed documents (e.g. reports) should be sent via **tracked post** from PPC offices or approved locations

6. Communication Standards

Method	Acceptable Practice	Not Acceptable
Text	Appointment confirmations, brief updates using initials only	Using full names or discussing detailed case information
Phone	Calls made in private; number withheld if preferred	Calls in public, open spaces, or while driving
Voice mail	Leave name and number only	Mentioning child/family names or reasons for the call
Email	Use encrypted email for sensitive information; use initials or first names only	Unencrypted sharing of reports, DOBs, or addresses
Photos/Videos	Taken only with signed consent and using work-designated devices	Using personal phones; storing media unprotected or unsupervised

7. Record Keeping and Note Management

- All clinical notes (paper or digital) must be accurate, dated, and stored securely
- Digital notes should be stored on cloud platforms that require a login and are GDPR-compliant
- SMS/email communications relevant to the case should be uploaded to the child's notes
- **Do not** store case notes as unsecured documents on local devices (e.g. Word files on desktop)

8. Use of Portable Devices and Media

- USB sticks, external hard drives, and discs may only be used if encrypted and stored securely
- Data should be transferred to secure storage and removed from portable devices promptly
- Never leave these items unattended or accessible to unauthorised individuals

9. Social Media and Professional Boundaries

- Do not follow, befriend, or interact with clients or families via social media platforms
- Avoid discussing or referencing clinical work on social media in any form
- Do not use **WhatsApp** or similar apps to share photos or videos with clients

10. Data Sharing and Third Parties

- Client data will only be shared with external professionals (e.g. schools, health teams) with **explicit consent**, unless there is a safeguarding risk
- Practitioners must:
 - Confirm consent in writing (e.g. email)
 - Ensure any shared data is proportionate and relevant
 - Use secure channels when sharing information

11. Data Retention and Disposal

- PPC retains records in line with professional guidelines:
 - For a minimum of **8 years** post-discharge
 - Or until the young person reaches the age of **26**—whichever is later
- After the retention period, records must be **securely destroyed or deleted**
- Practitioners must:
 - Use shredding or certified digital deletion
 - Maintain logs of disposed records if applicable

12. Breach Management

All suspected data breaches must be reported immediately to the designated Data Protection Officer, Mike Parsons (Managing Director). Affected individuals will be informed if appropriate, and the ICO will be notified within **72 hours** if a reportable breach has occurred.


13. Training and Review

- All staff and associates must complete regular data protection training
- PPC will review and update this policy **annually** or when legislative changes occur

14. Contact and Queries

For data protection queries or to report a concern, please contact:

Mike Parsons, Managing Director, Data Protection Lead – Phoenix Psychology Collective

 info@phoenixpsychologycollective.com