PRIVACY, DATA PROTECTION & CYBER SECURITY POLICY

Cairn Psychology Practice

HQ, 1 Berry Street, Aberdeen

Document Control & Version History

Version	Date	Author / Reviewer	Summary of Changes
1.0	November 2026	Dr Lesley Steptoe	Amalgamation of Clinical Notice and Forensic Court Security Policy.
1.1 (Planned)	November 2027	Dr Lesley Steptoe	Annual scheduled regulatory compliance review.

This Privacy Notice and Cyber Security Policy establishes how **Cairn Psychology Practice** collects, processes, archives, and destroys personal data and sensitive special category personal health data. All operations strictly comply with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and standard expert witness and clinical security protocols required across the Scottish courts, NHS, and Crown Office and Procurator Fiscal Service (COPFS). This practice is bound fully by Scots law under the exclusive jurisdiction of the Scottish courts.

1. Data Protection Overview & Contact Details

- **Data Controller:** Dr Lesley Steptoe operates as the formal Data Controller regarding all personal information, forensic records, and sensitive clinical data.
- **ICO Registration:** Dr Steptoe is a registered data controller with the Information Commissioner's Office under Registration Number: **ICO 00014950627**
- **Contact Channel:** All inquiries regarding data rights, Subject Access Requests (SARs), or data rectification must be submitted formally to: **info@cairnpsychologypractice.co.uk**

2. Cyber Security Architecture & Zero-Trust Environment

The practice operates a strict zero-trust data environment to ensure maximum protection for sensitive legal and clinical files:

- **Inbound Transmissions:** All incoming instructions, client medical files, tribunal papers, and legal disclosures must be transmitted exclusively via encrypted links or secure platforms such as Egress.

- **Practice Management:** Active case files, medical logs, and patient communication records are managed securely within WriteUpp, an industry-standard, GDPR-compliant platform utilizing 256-bit SSL encryption.
- **Diagnostic & Psychometric Tools:** Specialist diagnostic testing and psychometric scoring are processed through NovoPsych, ensuring health records are fully encrypted at rest and in transit.
- **Local Storage Security:** No sensitive clinical or forensic data is stored on unencrypted local devices or public cloud servers. Court bundles, psychometric materials, clinical notes, and draft reports are stored exclusively on encrypted, password-protected local hardware.
- **Cloud Backups:** Cloud backups use ISO 27001 certified storage located entirely within the UK.

3. Lawful Basis for Data Processing

Under the UK GDPR, the practice relies on specific legal pillars to process personal, health, and criminal allegation data:

Personal & Administrative Data (Article 6)

- **Article 6(1)(b) - Contractual Obligation:** For processing incoming instructions and managing individual therapy contracts.
- **Article 6(1)(c) - Legal Obligation / Administration of Justice:** For processing forensic instructions and fulfilling court requirements.
- **Article 6(1)(f) - Legitimate Interests:** For the commercial administration of the practice, including tracking calendar scheduling, managing invoicing systems, and processing payment logs.

Special Category & Criminal Data (Article 9)

Medical files and forensic bundles constitute special category data and may include details of criminal allegations. These are processed under:

- **Article 9(2)(h) - Health or Social Care:** For collecting and analyzing psychiatric symptoms, clinical histories, medical backgrounds, and psychometric profiles required to safely deliver clinical psychological treatment.
- **Article 9(2)(f) - Establishment, Exercise, or Defence of Legal Claims:** For processing records related to court instructions, expert reports, or legal disputes before the Scottish courts.

4. Categories of Data Collected

To safely manage your care or execute legal instructions, data is organized into three distinct groups:

- **Personal Identifying Information:** Full legal name, date of birth (mandated to verify our absolute 18+ adult user threshold), residential address, contact telephone number, and secure personal email address.

- **Special Category Clinical Information:** Medical practitioner details (GP name and surgery), active clinical symptoms, psychological histories, psychiatric medication records, psychological test scores, formal treatment notes, and summaries of care.
- **Forensic & Legal Materials:** Court bundles, criminal allegations, tribunal papers, and legal disclosures provided by instructing parties.

5. Communication Channels & Restrictions

Data security relies heavily on the channels used. To prevent metadata leaks and preserve professional encryption boundaries, the practice enforces strict communication protocols:

- **Official Email Only:** All billing updates, booking amendments, reports, and documentation are processed strictly via info@cairnpsychologypractice.co.uk or secure file transfer.
- **Prohibition of Text and WhatsApp:** Cairn Psychology Practice enforces a zero-tolerance rule against informal communication channels. Text messages (SMS) and WhatsApp chats are strictly barred. Any incoming consumer messages via these lines will be immediately deleted unread and will not form part of the clinical file to prevent unsecured mobile synchronization risks.

6. Third-Party Data Sharing & Financial Processing

The practice values data minimisation. Your details are never sold or rented to external marketing systems. Data transmission is strictly confined to the following scenarios:

- **Financial Gateway Processing:** Electronic fee payments are processed via secure third-party billing utilities (such as Stripe) or bank networks (BACS). Only required metadata is shared; raw card or account information is never saved locally on practice devices.
- **Private Medical Insurance:** If explicitly authorised, invoicing details and treatment tracking metrics are shared with providers (e.g., Bupa, AXA, Aviva) to process claims.
- **Clinical Risk Exemptions:** Data may be shared without client consent strictly in cases of immediate severe self-harm or suicide risk, intent to cause physical harm to third parties, statutory safeguarding duties, or direct court orders issued by the Scottish courts.

7. Website Data, Cookies & Enquiries

- **Enquiry Collection:** The website enquiry form collects name, organisation (where relevant), email address, telephone number, type of enquiry, and message. No IP addresses, device/browser information, or browsing history logs are recorded.
- **Data Handling:** Enquiries are emailed to the practice and a backup copy is securely retained within the site content management system to prevent data loss. This copy is private and readable only by the practice.
- **Spam Filtering:** The form uses no third-party spam-checking services, ensuring your data is never shared with external companies.
- **Lawful Basis for Enquiries:** Processing is based on Consent (Article 6(1)(a)) and Explicit Consent (Article 9(2)(a)) for any health data typed into the free-text message box, granted by ticking a non-pre-ticked mandatory checkbox.

- **Retention of Enquiries:** Website copies of enquiries are automatically deleted after 12 months. If an enquiry leads to a clinical instruction or therapy, the data is transferred to a formal case file governed by the 10-year retention rule.
- **Cookies & Analytics:** This website sets no cookies for visitors and uses no analytics services, advertising pixels, or third-party tracking. Signing into the practice's own content management system sets a strictly necessary session cookie that applies only to the practice. Web host server logs are maintained independently by the host for security and diagnostics.

8. Data Retention & Secure Destruction

- **Active Proceedings:** For forensic or legal instructions, records are held for the duration of the instruction and until the final hearing, appeal window, or parole board decision has concluded.
- **Post-Case Archive:** In accordance with professional indemnity criteria and medico-legal clinical record rules under Scots law, all files (intake forms, medical sheets, treatment summaries, invoices, and court bundles) are securely held within an encrypted digital archive for exactly 10 years from the official date of file closure or clinical discharge.
- **Secure Destruction:** Upon reaching the 10-year mark, digital media is permanently destroyed via secure electronic wiping and file erasure. Any physical documentation is shredded by a certified confidential waste partner.

9. Your Statutory Legal Rights

Under the UK GDPR, individuals retain specific statutory rights regarding their archived profile:

- **Right of Access:** The right to obtain a full copy of your personal data and clinical folder via a formal Subject Access Request (SAR), responded to within one calendar month.
- **Right to Rectification:** The right to demand immediate updates to inaccurate personal data or demographic entries.
- **Right to Erasure:** You may ask for personal data to be deleted. However, this right is limited where records form part of a court instruction, expert report, or formal legal health record. Once evidence has been provided to a court or enters a professional medical archive, the practice cannot delete it prematurely, and the 10-year retention period applies. Enquiries that did not lead to an instruction or therapy can be deleted upon request.
- **Right to Restriction:** The right to restrict processing if a contractual or legal dispute is active before the Scottish courts.
- **Withdrawing Consent:** Where processing rests on consent (e.g., website enquiries), you may withdraw it at any time to stop further use of that information.
- **Complaints:** If you are dissatisfied with how your data has been handled, please raise it with the practice first via the official email. You also retain the right to complain directly to the Information Commissioner’s Office at ico.org.uk or by telephone on 0303 123 1113.

10. Out-of-Hours Crisis Support Warning

Our digital email infrastructure and secure communication channels are monitored during business hours only for administrative tracking. **They must never be used for crisis communication.**

If an immediate safety emergency occurs post-discharge or outside of session times, you must contact local public emergency services directly:

- **NHS 24:** Call 111
- **Breathing Space Scotland:** Call 0800 83 85 87
- **Emergency Services:** Call 999 immediately