

CONFIDENTIALITY POLICY

Clinical Psychology & Employee Wellbeing Practice

1. Introduction and Commitment

The Origami Group is committed to maintaining the highest standards of confidentiality in accordance with UK legislation, professional ethical codes, and best practice guidelines. We recognise that confidentiality is fundamental to building trust and ensuring effective therapeutic relationships.

This policy applies to all staff members, contractors, volunteers, students, and anyone who may have access to client information within our practice.

2. Legal Framework

Our confidentiality practices comply with:

- General Data Protection Regulation (UK GDPR) 2018
- Data Protection Act 2018
- Human Rights Act 1998
- Mental Capacity Act 2005
- Children Act 1989/2004
- Professional body ethical guidelines (BACP, BPS, UKCP, HCPC)

3. Scope of Confidentiality

3.1 What is Confidential

All information relating to clients is considered confidential, including:

- Personal details and contact information
- Clinical notes and assessments
- Treatment plans and progress notes
- Correspondence regarding the client
- The fact that someone is receiving services from our practice
- Audio/video recordings (where applicable)
- Information about missed or cancelled appointments

3.2 Employee Assistance Programme (EAP) Considerations

For employee wellbeing services, we maintain strict separation between individual therapeutic work and any organisational reporting, ensuring employee confidentiality is protected even when services are employer-funded.

4. Information Sharing and Disclosure

4.1 Routine Sharing

Information may be shared in the following circumstances:

- **Within the clinical team** for supervision, case consultation, and continuity of care
- **With other healthcare professionals** involved in the client's care, with explicit consent
- **For training purposes** using anonymised case material

4.2 Disclosure Without Consent

We may disclose confidential information without consent only when:

- **Risk of serious harm** to the client or others exists

CONFIDENTIALITY POLICY

- **Child protection concerns** arise
- **Court orders** or legal obligations require disclosure
- **Prevention of terrorism** under relevant legislation
- **Public health emergencies** where disclosure is mandated

4.3 Risk Assessment and Disclosure Decisions

When considering disclosure without consent, we will:

- Assess the severity and immediacy of risk
- Consider whether disclosure is proportionate and necessary
- Consult with supervisors or senior clinicians where possible
- Document the decision-making process
- Inform the client of the disclosure where safe and appropriate to do so

5. Client Rights and Consent

5.1 Informed Consent

Clients will be informed about:

- How their information will be used and stored
- Who may have access to their information
- Circumstances where confidentiality may be breached
- Their rights regarding their personal data
- How to access or correct their information

5.2 Ongoing Consent

We obtain explicit consent for:

- Sharing information with GPs or other healthcare providers
- Using case material for training or research
- Audio/video recording of sessions
- Involving family members or carers in treatment
- The utilisation of specific AI related tools to enhance our practice

5.3 Data Subject Rights

Under UK GDPR, clients have the right to:

- Access their personal data
- Correct inaccurate information
- Request deletion of data (where legally permissible)
- Restrict processing of their data
- Data portability
- Object to processing

6. Data Storage and Security

6.1 Physical Security

- Client files stored in locked cabinets
- Restricted access to clinical areas
- Clean desk policy implemented
- Secure disposal of confidential waste

CONFIDENTIALITY POLICY

6.2 Digital Security

- Password-protected systems and devices
- Encrypted storage and transmission
- Regular security updates and backups
- Access controls and audit trails
- Secure email systems for client communication

6.3 Retention Periods

- Adult client records: 7 years from last contact
- Child/adolescent records: Until 25th birthday or 7 years from last contact (whichever is longer)
- Employment records: 6 years from termination
- Safeguarding records: May be retained longer as required

7. Special Circumstances

7.1 Minors and Young People

- Parents/guardians normally have access to children's records
- Gillick competent young people (typically 16+) may consent to confidential treatment
- Best interests of the child is always paramount
- Clear protocols for involving parents/carers

7.2 Adults Lacking Capacity

- Decisions made in best interests under Mental Capacity Act
- Involvement of lasting power of attorney holders or court-appointed deputies
- Consultation with family members and care teams as appropriate

7.3 Deceased Clients

- Duty of confidentiality continues after death
- Disclosure only with executor consent or legal requirement
- Consideration of impact on surviving family members

8. Third-Party Information

Information shared by clients about third parties is also treated confidentially unless:

- Serious risk of harm exists
- Legal obligations require disclosure
- The third party has consented to sharing

9. Training and Supervision

9.1 Staff Training

All staff receive training on:

- Confidentiality requirements and procedures
- Data protection obligations
- Risk assessment and disclosure decisions
- Information security measures

9.1(b) Consultant Clinicians

CONFIDENTIALITY POLICY

All consultant clinicians are expected to maintain their own training on the above subjects.

9.2 Clinical Supervision

- Regular supervision includes confidentiality considerations
- Anonymous case discussion where possible
- Clear guidelines for supervisor access to client information

10. Complaints and Breaches

10.1 Reporting Breaches

Staff must immediately report any:

- Suspected or actual confidentiality breaches
- Data protection incidents
- Security concerns

10.2 Breach Response

- Immediate containment and risk assessment
- Investigation and documentation
- Client notification where appropriate
- Reporting to Information Commissioner's Office (ICO) if required
- Implementation of preventive measures

10.3 Client Complaints

Clients may raise confidentiality concerns through:

- Our internal complaints procedure
- Professional body complaints processes
- Information Commissioner's Office
- Care Quality Commission (where applicable)

11. Multi-Agency Working

When working with other agencies:

- Clear information sharing agreements in place
- Roles and responsibilities defined
- Consent obtained for specific sharing arrangements
- Regular review of sharing arrangements

12. Technology and Remote Services

12.1 Teletherapy and Video Consultations

- Secure platforms used for remote sessions
- Client consent obtained for remote delivery
- Privacy and confidentiality maintained during remote sessions
- Clear guidance on technical requirements and limitations

12.2 Communication Channels

- Secure email systems for client contact

CONFIDENTIALITY POLICY

- Encrypted messaging where appropriate
- Clear policies on social media and informal contact

13. Policy Review and Updates

This policy is reviewed annually and updated as necessary to reflect:

- Changes in legislation
- Professional guidance updates
- Lessons learned from incidents
- Best practice developments

14. Contact Information

For questions about this policy or confidentiality concerns:

- Practice Manager: Mireille Bernadac
- Data Protection Officer: Mireille Bernadac
- Senior Clinical Lead: Amy Stoddard-Ajayi

Information Commissioner's Office: 0303 123 1113 or ico.org.uk

Policy Version: 1.0

Approved by: Amy Stoddard-Ajayi

Role: CEO and Founder

Date of Approval: 07/07/2025

Next Review Due: 07/07/2026

This policy should be read in conjunction with our Data Protection Policy, Information Security Policy, and relevant professional codes of conduct.