Origami Group

USE OF IT IN BUSINESS POLICY

Clinical Psychology & Employee Wellbeing Practice

1. Purpose

This policy outlines the appropriate use of information technology (IT) systems within Origami Group to support secure, ethical, and professional operations in line with our clinical responsibilities, UK legislation, and industry standards, including the General Data Protection Regulation (UK GDPR) and guidance from the Information Commissioner's Office (ICO).

2. Scope

This policy applies to all staff, contractors, associates, and volunteers who use IT systems and devices on behalf of the Origami Group whether onsite, remotely, or via personal equipment accessing company resources.

3. Acceptable Use

- IT resources must be used solely for business purposes, including client communication, administrative tasks, clinical documentation, supervision, and research.
- All use must comply with confidentiality, data protection, and clinical best practices.
- Access to client records and sensitive information must be conducted through secure, authorised platforms (e.g. encrypted practice management systems).

4. Security and Data Protection

- All devices accessing client or business data must be protected with secure passwords and, where possible, multi-factor authentication.
- Staff must not download, store, or transfer identifiable client information on personal devices without explicit authorisation and appropriate encryption.
- All data processing must comply with UK GDPR and the Origami Group's **Data Protection and Confidentiality Policy**.
- Regular system updates, antivirus software, and firewalls must be maintained.

5. Email and Communication

- Staff must use official, secure email accounts provided by Origami Group for all client-related correspondence.
- Emails containing sensitive information must be encrypted or password-protected if required.
- Instant messaging or social media platforms must not be used to communicate with clients unless specifically authorised and covered under safeguarding protocols.

6. Remote Work and Cloud Services

- Remote access must only occur via approved, secure platforms (e.g., encrypted VPN or secure cloud-based systems).
- Staff must not use public Wi-Fi for accessing practice systems without a secure connection (VPN).
- Cloud services used must meet UK data sovereignty standards and be GDPR-compliant.

7. Monitoring and Compliance

- The practice reserves the right to monitor the use of IT systems to ensure compliance with this policy and other relevant policies.
- Any breaches or suspected breaches (e.g., data leaks, unauthorised access) must be reported immediately to the Data Protection Officer or designated lead.

USE OF IT IN BUSINESS POLICY

8. Personal Use

- Limited, reasonable personal use of IT resources is permitted outside of clinical hours, provided it does not interfere with business operations or contravene professional standards.
- Personal use must never involve accessing or storing client data.

9. Training and Awareness

- All staff must receive IT and data protection training during induction and at regular intervals.
- Awareness of cyber threats (e.g., phishing, ransomware) is essential, and staff should follow guidance to mitigate risks.

10. Disciplinary Action

- Breaches of this policy may result in disciplinary action, including potential termination of contracts or referral to professional regulatory bodies where applicable.

11. Review and Updates

This policy will be reviewed annually or in response to changes in legal, regulatory, or operational requirements.

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