Policy title:	**IT Policy**

Summary:	This policy outlines the acceptable use, management, and governance of IT resources, systems, and artificial intelligence (AI) tools within Insight Psychological Assessments Ltd, a UK-based psychological assessments provider. It ensures that information systems are secure, compliant with legal and ethical standards (including GDPR and HCPC guidelines), and support the safe use of AI in clinical, research, and administrative contexts.
Target audience:	All Insight Assessments '*team members*', whether employed, contracted or part-time, paid or unpaid, volunteers, students, and contractors.
Authorised by:	Insight Psychological Assessments Ltd Director
Date issued:	1st September 2025
Next review date:	31st August 2026

Version no.	Issue date	Summary of amendments

1. Scope

This policy applies to:

- All employees, contractors, interns, and affiliates of Insight Psychological Assessments Ltd
- All devices and systems used to access company data
- All platforms including cloud services, AI tools, email, and telehealth systems
- All clients, including corporate partners, NHS affiliates, and private patients

2. Legal and Regulatory Compliance

Insight Psychological Assessments Ltd complies with:

- **UK GDPR (General Data Protection Regulation)**
- **Data Protection Act 2018**
- **Health and Care Professions Council (HCPC) Standards of Conduct, Performance and Ethics**
- **NHS Digital (if applicable)**
- **ICO (Information Commissioner's Office) Guidance**
- **The Equality Act 2010**

3. Data Protection and Confidentiality

3.1 Patient and Client Data

All personal and sensitive data, especially clinical assessments and reports, must be:

- Stored securely (encrypted at rest and in transit)
- Accessed only by authorised individuals on a need-to-know basis

3.2 Data Storage

- Use only company-approved platforms (e.g., Microsoft 365, encrypted cloud services)
- No local storage of client data on personal devices
- Backups must be automatic, encrypted, and stored within the UK or an approved jurisdiction (as per GDPR)

4. Use of Artificial Intelligence (AI)

4.1 AI in Clinical Settings

- AI will not be used to make autonomous clinical decisions

- All outputs from AI tools (e.g., psychological scoring algorithms, report summarisation, transcription) are reviewed and validated by a qualified clinician
- AI use is explainable, transparent, and used in accordance with HCPC guidelines and clinical best practice

4.2 Approved AI Use Cases

- Drafting clinical reports (e.g., summarising findings — with clinician oversight)
- Automating scheduling, transcription, or form completion
- Anonymising or pseudonymising client data for training or research purposes
- Internal decision support tools (e.g., workload management, risk scoring — with human review)

4.3 Restrictions on AI

- Do not use public AI tools (e.g., ChatGPT, Google Bard) for entering client-identifiable data
- Only use AI tools that have been vetted by the company's Data Protection Officer (DPO) or IT Lead

5. Information Security

5.1 Device Usage

- All company devices must be password-protected and encrypted
- Multifactor authentication (MFA) is mandatory for cloud access

5.2 Remote Working

- Ensure confidentiality of conversations and screens during client sessions
- Store no files locally on personal devices unless explicitly authorised

5.3 Email and Communications

- Avoid sending sensitive data via email unless password protected or encrypted (e.g., using Egress)
- Do not use personal messaging apps for client communication

6. Monitoring and Audit

Insight Assessments reserves the right to monitor IT systems to ensure compliance with this policy. This includes:

- Email and file usage logs
- Access logs to client data
- AI tool interactions (where applicable)

Monitoring will be proportionate and respect privacy rights, in line with the Regulation of Investigatory Powers Act 2000 (RIPA) and GDPR.

7. Training and Awareness

- All employees and self-employed consultants engaged by the company must complete mandatory IT security and data protection training on an annual basis.

- Self-employed consultants are responsible for ensuring their knowledge of IT security, data protection, and relevant regulatory requirements remains current, and must be able to evidence compliance if requested.

- Where consultants make use of AI tools in clinical or research contexts, they are responsible for maintaining up-to-date knowledge of AI literacy, ethical considerations, and professional standards relevant to their practice. Consultants must be able to demonstrate that they have undertaken suitable continuing professional development in this area.

- The company may from time to time signpost external resources to support consultants in meeting these obligations, such as:

    - Guidance from the British Psychological Society on digital competence and ethical practice

    - Information Commissioner's Office resources on AI and data protection

    - NHS AI Lab materials on safe and ethical use of AI in healthcare

    - Recognised CPD platforms offering AI literacy or ethics courses (e.g. FutureLearn, Coursera, LinkedIn Learning)

    - It remains the responsibility of each consultant to select appropriate training, ensure it is relevant to their professional role, and maintain evidence of completion.

8. Policy Violations

Breaches of this policy may result in disciplinary action, up to and including termination of contract for services and legal prosecution, depending on the severity.