HARK & SPARK

• PLAY • LISTEN • SPEAK •

Information Handling & Confidentiality Policy

1.1 Purpose: Hark & Spark is committed to ensuring that confidential, person-identifiable information (client details, clinical notes, and medical histories) in any medium is collected, stored, and transmitted safely with maximum security.

1.2 Scope: Applies to all clinical, administrative, and financial information managed by the business, whether operating from a main office, clinical space, working from home, or during mobile community visits.

1.3 Written and Verbal Disclosures: Clinical conversations or telehealth sessions must always be conducted in private environments where they cannot be overheard by unauthorised parties.
Public spaces (such as cafes or public transit) will never be used to work on identifiable client documents unless they have been fully anonymised first.

1.4 Secure Digital Practices: Client records must be accessed and managed electronically through secure, approved clinical cloud systems rather than physical printouts.
If highly sensitive data must be emailed for practical clinical reasons, it will never be included in the main body of the email; it must be sent within an attached, password-protected, encrypted document, with the password provided to the recipient via a separate communication channel.
Direct forwarding of identifiable client data to personal, unencrypted email accounts or devices is strictly prohibited.

1.5 Quality Assurance: Self-directed confidentiality audits will be conducted bi-annually to review access logs, ensure data integrity, and evaluate the ongoing security controls of all business infrastructure.

Last reviewed: 25.05.2026