



Data Protection and Security Policy

Keeping your personal information safe is extremely important to me. This policy explains how I protect your data, the security measures I use, and the steps I take to ensure your information is handled lawfully, respectfully and securely at every stage of our work together.

This policy supports my Privacy Policy and applies to all personal data collected, stored or processed during counselling — whether in person, online or by telephone.

1. Legal Responsibilities

I follow all current UK data protection legislation, including:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Privacy and Electronic Communications Regulations (PECR)
- Counselling Information Regulations (2025)
- Online Safety Act (2023–2024 rollout)

I am registered with the Information Commissioner's Office (ICO): ZB925023.

As the data controller, I am responsible for keeping your information safe and deciding how it is used.

2. How Your Data Is Stored and Protected

I use several layers of security to protect your information:

Zero-Knowledge Encryption (Primary Security Method)

All digital records — including personal details, session notes, safeguarding records, emails saved for clinical purposes, and any documents relating to your therapy — are stored using zero-knowledge encrypted software.

This means:

- Your data is encrypted in a way that only I can access.
- No external provider, platform or cloud service can view, decode or read your information.
- Even if the storage provider were compromised, your data would remain unreadable.

This is one of the highest levels of data protection available and exceeds minimum professional requirements.

Device Security

- All devices are password-protected and use multi-factor authentication.
- Software is kept updated to maintain security.
- No client information is stored on portable devices unless encrypted.

Paper Records

- Any paper documents (rare) are stored in a locked cabinet.
- Only I have access to the key.

3. Communication Security

To protect your confidentiality:

- Emails are sent through secure, encrypted systems.
- Sensitive information is not shared by text, WhatsApp or social media.
- Text messages and emails are deleted within 24 hours unless clinically necessary.
- Online sessions take place on secure, encrypted platforms.
- You are encouraged to join online sessions from a private, safe space.

4. Access to Your Information

Only I have access to your personal information.

I do not:

- share your data with third-party processors
- transfer your data outside the UK
- use automated decision-making or profiling

Information is only shared when legally required or necessary to prevent serious harm.

5. Retention and Deletion

Your records are kept securely for:

- 7 years after counselling ends, or
- until a child reaches age 25, whichever is longer.

After this, all data is permanently and securely destroyed.

You may request earlier deletion unless I am legally required to retain your information.

6. Your Rights

You have the right to:

- access your personal information
- request corrections
- request deletion (where legally appropriate)
- request limits on how your data is used
- understand how long your data is stored
- know who it may be shared with

Requests can be made by emailing: nic@thelistening-ear.co.uk

I respond within 14 working days.

7. Data Breaches

If a data or confidentiality breach occurs:

- I will investigate and record the incident.
- You will be informed if your information is affected.
- I will notify the ICO if required.

8. Confidentiality After Death

Your confidentiality continues after your death.

My clinical will executor ensures your records are handled securely and respectfully.