

Privacy Policy –

My Space Counselling is committed to complying with the terms of the General Data Protection Regulation (GDPR) and to the responsible and secure use of your data. My Space Counselling has a legitimate interest in processing personal data to provide counselling services. The purpose of this statement is to let you know what personal information My Space Counselling, collects and holds, why We/I collect this data, how long it is stored for and your rights over your personal data. My Space Counselling is registered with the Information Commissioner's Office (ICO).

1. Information about you

1.1 I/we collect personal information from you when you enquire about our counselling services to set up an initial appointment. This information includes contact details, your availability and other relevant personal information, including emergency contact information (Please ensure that the named contact is aware that their information is being shared). Once a client finishes Counselling, all data regarding their Counselling is stored securely for 7 years (Or the time you state) and then destroyed.

1.2 When you enquire about Counselling, we ask for contact details and relevant personal information from you that is needed to answer your enquiries and to keep you informed.

2. Our use of this information

2.1 Your data will be used only to provide you with Our/My services and to give you information relating to Our/My services. I/we will not share your details with any other person or organisation without your knowledge and permission unless there is a legal requirement as stated in the counselling contract or (exceptions you may have). A breach of confidentiality is when a person shares information with another in circumstances where it is reasonable to expect that the information will be kept confidential.

3. Security

3.1 I/We will take all reasonable precautions to prevent the loss, misuse, or alteration of information you give us.

3.2 Communications in connection with this service may be sent by email. For ease of use and compatibility, communications will not be sent in an encrypted form unless you require it and give Me/Us permission to communicate with you in that way. Email, unless encrypted, is not a fully secure means of communication. Whilst I/We endeavour to keep our systems and communications protected against viruses and other harmful effects, we cannot bear responsibility for all communications being virus-free.

4. Your rights over your personal data

4.1 If you would like to see the information, we hold about you, or would like to correct, update, or delete any records, please email me.

4.2 If you have a concern or questions about how My Space Counselling handles data, you can raise it with me directly by emailing myspacecounselling@outlook.com. I will

acknowledge your complaint within 30 days, investigate it without undue delay, keep you informed of the progress, and let you know the outcome. You can contact Information Commissioner's office at anytime: ico.org.uk

My Space Counselling is ICO registered. Trainees and Counsellors on the Referral Pathway also have their own individual ICO registration.

How we store client information:

- WriteUpp Clinical Software (Qualified Counsellor Records)

In accordance with the UK Data (Use and Access) Act 2025 and UK GDPR requirements, I have assessed WriteUpp as the clinical records system used to store client session notes, assessments, contracts, and contact information. My assessment considered the platform's security features, data protection compliance, access controls, storage arrangements, confidentiality safeguards, and suitability for counselling practice. WriteUpp is used to support secure record-keeping and continuity of care, with access restricted to authorised users and appropriate technical and organisational measures in place to protect client data. I am satisfied that its use is proportionate, necessary, and consistent with my professional and legal responsibilities regarding client confidentiality and data protection.

Write Upp is **ISO 27001 Certified - Secure & GDPR-compliant records within a fully secure system that respects client privacy:**

- GDPR compliance and ISO27001 certification ensure the highest standards of data protection.
- Over a decade of trusted service to NHS therapy providers.
- Two-factor authentication (2FA) for an added layer of security.

www.writeupp.com

Digital tools are periodically reviewed as part of our ongoing data protection and confidentiality responsibilities.

- Google Drive (Trainee Counsellor Client Information)

In accordance with the UK Data (Use and Access) Act 2025 and UK GDPR requirements, I have assessed Google Drive as a digital tool for the secure storage and sharing of client-related information used in trainee counselling practice. My assessment considered data security measures, encryption, access controls, confidentiality requirements, data processing arrangements, and the necessity and proportionality of its use. Appropriate safeguards are in place, including restricted access, password protection, and the minimisation of personal data.

Microsoft OneDrive helps ensure the security and confidentiality of stored information through several layers of protection:

1. Encryption

- **In transit:** Files are encrypted using TLS/SSL when moving between your device and Microsoft's servers.
- **At rest:** Files stored in OneDrive are encrypted on Microsoft's servers using strong encryption technologies (such as AES-256).

2. Access Controls

- Users must authenticate with a Microsoft account or organizational credentials to access files.
- Permissions can be set to control who can view, edit, or share files.
- Shared links can be restricted with passwords, expiration dates, or specific recipient access (depending on the account type).

3. Multi-Factor Authentication (MFA)

- OneDrive supports MFA, requiring a second verification method in addition to a password, significantly reducing the risk of unauthorized access.

4. Version History and Recovery

- Previous versions of files can be restored if files are accidentally changed, corrupted, or affected by ransomware.
- Deleted files can often be recovered from the recycle bin within a retention period.

5. Ransomware Detection and Protection

- OneDrive can detect unusual file activity that may indicate ransomware and help users recover affected files.

6. Microsoft Security Infrastructure

- Data centers are protected by physical security measures, continuous monitoring, and security operations teams.
- Microsoft regularly audits its systems and complies with many international security and privacy standards.

7. Personal Vault

- OneDrive offers a feature called Personal Vault that provides an additional layer of identity verification for especially sensitive files.

8. Compliance and Privacy Controls

- For business and enterprise users, OneDrive integrates with Microsoft 365 security and compliance tools, including data loss prevention (DLP), retention policies, auditing, and information protection features.

Best Practices for Users

Even with OneDrive's protections, confidentiality also depends on user actions:

We endeavour to:

- Use a strong, unique password.
- Enable MFA.
- Review sharing permissions regularly.
- Avoid sharing sensitive files through public links.
- Keep devices updated and protected with antivirus software.

No cloud storage service can guarantee absolute security, but OneDrive combines encryption, access controls, monitoring, and recovery features to provide a strong security framework for stored information.

I am satisfied that to the best of our intentions Google Drive can be used in a manner that supports the confidentiality, integrity, and security of client information.

Digital tools are periodically reviewed as part of our ongoing data protection and confidentiality responsibilities.

Trainees use codes as a means of identifying clients within their notes. They comply with the policies and procedures as set out by their training provider / college. Trainees can share these policies with yourselves if you wish.

Supervision

In the UK, counselling supervision complies with confidentiality by balancing **client privacy** with the need for **professional oversight and safe practice**.

Key ways this is achieved include:

1. Confidentiality Agreements

Counsellors and supervisors are bound by professional and ethical codes that require them to keep information confidential. Supervisors treat information discussed in supervision with the same level of confidentiality as counsellors treat client information.

2. Limited Disclosure of Client Information

When discussing cases in supervision, counsellors are encouraged to:

- Avoid using full names or identifying details.
- Use pseudonyms or initials where possible.
- Share only the information necessary for the supervisory purpose.

This helps protect client anonymity while allowing meaningful discussion of the work.

3. Informed Consent

Many UK counselling services inform clients that counsellors receive supervision and that aspects of their work may be discussed confidentially with a supervisor. This is often included in the counselling contract or privacy notice at the start of therapy.

4. Data Protection Compliance

Supervision records and client information must be handled in accordance with UK data protection law, including the UK General Data Protection Regulation and the Data Protection Act 2018. Records should be stored securely, whether electronically or on paper.

5. Professional Ethical Frameworks

Professional bodies such as the British Association for Counselling and Psychotherapy, National Counselling and Psychotherapy Society, and UK Council for Psychotherapy require members to have supervision and maintain confidentiality within that process.

6. Exceptions to Confidentiality

As with counselling itself, confidentiality in supervision is not absolute. Information may need to be disclosed if there are concerns about:

MY SPACE COUNSELLING

- Serious risk of harm to the client or others.
- Safeguarding concerns involving children or vulnerable adults.
- Terrorism-related concerns or other legal obligations.
- Court orders or statutory requirements.

Where possible, clients are informed about these limits to confidentiality at the outset of counselling.

Example

A counsellor might tell a supervisor:

"I'm working with a client in their thirties who is experiencing anxiety following a relationship breakdown."

Rather than:

"I'm working with Sarah Jones from Exeter, who lives on..."

The first example provides sufficient information for supervision while protecting the client's identity.

In summary, supervision supports safe and effective counselling practice while preserving confidentiality through anonymisation, professional ethics, informed consent, secure record-keeping, and adherence to UK legal and regulatory requirements.