

Online Counselling Safety: A Quick Client Guide

Online therapy (via video, chat, or email) offers convenience and accessibility, but protecting your privacy and personal data requires a few simple precautions. Use this fact sheet to ensure your sessions remain secure and confidential.

1. Secure Your Hardware & Network

- **Use a Private Device:** Whenever possible, join sessions from a personal computer, tablet, or phone. Avoid using work-issued devices, library computers, or shared family hardware.
- **Avoid Public Wi-Fi:** Coffee shop or airport Wi-Fi networks are often unencrypted. Always connect via a password-protected home network or a trusted mobile hotspot.
- **Keep Software Updated:** Regularly update your device's operating system, web browser, and video platform app to ensure you have the latest security patches.

2. Protect Your Physical Environment

- **Choose a Private Space:** Select a room where you can close the door and speak freely without being overheard.
- **Manage Headphones:** Using wired or trusted Bluetooth headphones keeps your therapist's voice private and reduces audio bleed.
- **Mind Your Background:** If using video, check what is visible behind you. Most platforms offer a **blurred background** feature if you want to keep your personal space hidden.

3. Verify Your Practitioner & Platform

- **Confirm Platform Security:** Ask your therapist if their platform is compliant with local health privacy standards (e.g., HIPAA in the US, GDPR/NHS standards in the UK). Standard consumer apps like standard FaceTime or regular Skype may not meet these requirements.
- **Check End-to-End Encryption:** Ensure video or messaging tools use end-to-end encryption so third parties cannot intercept your session.
- **Verify Credentials:** Confirm that your practitioner is licensed or registered with a recognized professional body (e.g., BACP, UKCP, APA) before sharing sensitive personal details.

4. Practice Good Digital Hygiene

Action	Best Practice
Passwords	Use strong, unique passwords for your client portal/email accounts. Enable Two-Factor Authentication (2FA) if available.

Session Links	Never share session URLs or meeting IDs on social media or in public forums.
Email/Texting	Avoid sending detailed clinical information via standard email or SMS unless encrypted; save deep discussions for the session.
Recordings	Neither you nor your therapist should record sessions without explicit, prior written consent from both parties.

Emergency Note: Online therapy is generally intended for scheduled, non-emergency support. If you are experiencing an immediate crisis or emergency, contact your local emergency services (e.g., 999 or 911) or a dedicated crisis hotline right away.