College of Sexual and Relationship Therapists

Online therapy and supervision

Online therapy and supervision

1. Training is recommended to provide a professional service when working online.
2. It is not assumed that a Member competent in working face to face will automatically have competence working online. Additionally, because of the wide-ranging issues that are likely to be brought to online therapy, it is recommended that it is only conducted by clinically experienced Members. Possible advantages and disadvantages of online therapy need clarification with the Service user prior to commencing therapy. These might include the lack of visual and auditory cues, security issues and possible limitations to, and errors in using technology. Members are reminded to make sure that they have suitable insurance cover for this work.
3. Technological competence is necessary and Members considering working online have a responsibility to ensure they have sufficient up-to-date technological knowledge as well as therapeutic experience.
4. Members should also ensure that the Service user has an adequate understanding of the technological issues involved, including limitations, risks, threat to privacy etc. Privacy of data is maintained by the use of encryption and appropriate access control for all drives, files and communication systems and by firewall and virus protection for computers.
5. If the Member is not completely confident of the security of any storage or communications mechanism, it is inadvisable to proceed with working in this way.
6. Security should be regularly reviewed and updated. The service user should be kept advised of any security limitations so that they can give an informed consent.
7. Supervision of online work from someone who is trained and experienced in working online is advisable. The supervisor should have an extensive understanding of the complexities of online work. Both supervisor and Member should be aware of the need to protect personal data and to obtain explicit consent to the sharing of data.
8. Knowledge of law relevant to the Service user's geographical location needs to be understood and complied with, including the right to practice. If the therapy is being provided within the UK then the law of the UK prevails. Members are bound by the COSRT Code of Ethics and Practice for General and Accredited Members regardless of the location of the service user.
9. The Member must also make sure that they are not in breach of any local law where a Service user is outside the UK. Other applicable laws that may be considered are the Data Protection Act 2018, the Customer Contracts Regulations 2013, the Privacy and Electronic Communications Regulations 2003 (as amended) and the Freedom of Information Act 2000

(Commencement No. 4) Order 2004, and any other such legislation which may from time to time come into force. For the purposes of data protection, personal data may not be transferred outside the EEA.

10. Assessment of Service users for online work is essential. This ensures that where there are limitations or exceptions to the advisability of working online, appropriate referrals are made either online or within the Service user's geographical area. Some conditions may not be suitable for online work and again appropriate referral should be sought. Reasonable steps must be taken regarding the protection of the identity of the Service user.
11. Contracting should be clear and cover all the issues addressed in COSRT guidance. It should be available on the Member's website either as a download document or information page and should contain information about how email addresses, credit card information and the Service user's records are used, shared, stored and eventually deleted. Language should be unambiguous and clear to avoid confusion. Particular attention needs to be paid to boundaries to online contact, such as response times to emails.
12. The terms of use of the Member's online service should be available to Service users. It should include the Member's geographical location and how they can be contacted, whether through a postal address, telephone or email.
13. There must be agreement about how to proceed in the event of a technology breakdown or other disconnection occurring during a session.
14. The contract also outlines the possible risks of the use of insecure communications or storage methods, such as unencrypted email, that the Service user may elect to use.
15. Informed consent is part of the contract and should be obtained prior to starting work with a Service user.
16. Steps must be taken to ascertain whether parental consent is needed.
17. For the purposes of data protection, minors can give consent to the use of their personal data from the age of thirteen.
18. Confidentiality is best maintained in all electronic communications by Members ensuring that as little sensitive or personally identifiable material as possible is stored or transmitted and, if it is, that it is stored or transmitted securely.
19. All measures possible must be taken to protect sensitive information and Members must constantly be alert to the potential risk of a third-party gaining access to information. As part of the assessment it should be considered whether a third party might have a vested interest

in accessing information e.g. domestic violence. If online therapy is considered inappropriate because of this, onward referral should be sought.

20. Password protection may be used in forums and these should be changed at regular intervals