Working online in the counselling professions

Contents

Context

This resource is one of a suite prepared by BACP to enable members to engage with BACP's *Ethical Framework for the Counselling Professions* regarding digital technology.

Using Fact Sheet Resources

Fact Sheet resources support good practice by offering additional guidance in respect of ethical principles and policy applicable at the time of publication. These resources should be used in conjunction with BACP's *Ethical Framework for the Counselling Professions.* They are not intended to be sufficient for resolving specific issues or dilemmas arising from work with clients, which are often complex. In such situations, we recommend consulting a suitably qualified lawyer or practitioner.

Specific issues in practice will vary depending on clients, particular models of working, the context of the work and the kind of therapeutic intervention provided. Please be alert for changes that may affect your practice, as organisations and agencies may change their practice and policies. All references in this document were up to date at the time of writing but there may be changes to the law, government departments, websites and web addresses that affect you, so it is important for you to keep informed of these.

1 Working online

Working online involves a distinct set of ethical challenges – some similar to working face to face and others unique to this way of communicating with clients at a distance from you. In all cases the established values, principles and personal moral qualities provide useful points of reference for thinking through the issues involved.

The *Ethical Framework for the Counselling Professions*, states that:

We will fulfil the ethical principles and values set out in this Ethical Framework regardless of whether working online, face to face or using any other methods of communication.

The technical and practical knowledge may vary according to how services are delivered but all our services will be delivered to at least fundamental professional standards or better (Good Practice, point 20).

'Working online' is used in this guidance to include all methods of communication using digital and information technology regardless of whether equipment used is a desktop computer, laptop, tablet, smartphone or any other device. 'Working online' is also sometimes referred to as 'working at a distance' to establish a distinction from working in the physical presence of the other person.

The main focus of this guidance is exploring some of the key issues involved in meeting the ethics and standards for working online, with particular regard to services for clients or closely related activities.

2 Variations in use of online and digital technology

Digital and online resources are widely used by the counselling professions and in society. Appointments may be arranged by email or text and managed using electronic calendars. Appointment reminders may be sent to clients electronically. Services to clients may be provided by a wide variety of online and digital communications including text, email, audio or video communications, or through social media. Records of sessions, invoicing and payments may be undertaken, and stored electronically. Working online can be undertaken from a seemingly ever-expanding range of devices.

3 Technological competence

- All practitioners should be sufficiently competent in the use of technology in their work to be able to provide reliable and adequate services to clients and colleagues.

- Basic competence includes having alternative ways of providing services for communicating with clients promptly if the primary method of communication fails; having access to technological support that respects the confidentiality of the work being undertaken; and, keeping up to date concerning new developments in the technology being used in order to provide the safest and most reliable service to clients.

- Competence in providing services that use unfamiliar technology are best supported by formal training from specialists or working in consultation with more experienced practitioners.

- It is considered good practice to receive at least some supervision online through similar technology to that used for working with clients (see Point 12 below).

4 Security and confidentiality

Absolute security in the digital world does not exist. Carefully considered decisions need to be made by:

- ensuring that services are accessible and acceptable to clients

- taking reasonable steps to ensure adequate levels of security for the type of service being provided, and

- being vigilant in avoiding new threats to security as they arise in a rapidly changing field of practice and technology.

Threats to security typically arise from using the wrong type of hardware or software, technological failures, the behaviour of people involved, or unauthorised intrusion by third parties. Sources of threat may include:

- **Physical intrusion** at either end of the communication, for example by being overheard or someone being present without the knowledge and consent of the person at the other end of the communication. Physical security needs to extend beyond the actual sessions by ensuring that the means of communication are adequately protected and not left open for others to view current transactions or to search for the history of communications. Practitioners are directly responsible for protecting their end of the communications.

Good practice safeguards against physical intrusion include vigilance about being overheard or overseen, adequate password protection and encryption of data to prevent intrusion on equipment and software used, and by providing information to clients about how best to protect their security.

- **Electronic intrusion** by third parties typically arises because of:

    – using insecure methods of communication including unprotected Wi-Fi

– inadequate firewalls and virus protection being used at either end of the communication

– security systems being bypassed by third parties, possibly by the use of spyware or code breakers, which may be readily available on the internet.

Good practice safeguards against intrusion by third parties include: adequate password protection and encryption of services being provided, regularly updating firewalls, virus protection or other applicable security systems and providing suitable information to service users to enable them to protect their end of the communications.

- **Electronic intrusion by the online communication provider** is to some degree unavoidable when using any of the platforms or applications that make online communications possible. However, there is a wide variation in how far providers of online and digital services intrude on the communications they transmit, claim ownership of what is communicated and the degree to which they protect the privacy of the communications they facilitate.

Free services have the advantage of no upfront cost and are likely to be the most familiar and accessible to both clients and practitioners alike. However, these positive features are counterbalanced by the provider usually depending financially on acquiring information about their users to market additional services, for which they can charge a fee, or to advertise other products. As a consequence, some free online services may offer poor levels of privacy or other safeguards. The absence of such safeguards may make them ethically unsuitable for work that involves communicating personally sensitive or health-related information to practitioners and their clients. It is important to have considered the terms and conditions of potential service providers and particularly their approach to protecting privacy and security. It is often worth conducting periodic searches online to see if there have been any reported breaches of privacy or security incidents involving potential providers. Recent scandals have revealed that promises of privacy and security are not always delivered in actual practice. As working online relies on rapidly changing technology, any system is only as good as its last update.

Good practice safeguards against electronic intrusion by the online communication provider include:

– using providers and electronic platforms that meet the privacy and quality standards for healthcare – especially when working with personally sensitive information

– carefully checking the provider's contractual terms and conditions to ensure that they are suitable for the type of service being provided

– offering more secure alternatives to clients where this is practicable

– keeping up to date with new developments to enhance the privacy, security and reliability of your chosen method of communication.

• **Electronic surveillance** by national security services is a feature of contemporary life. Practice varies between countries in how they balance the protection of public safety against electronic intrusion on private communications. In so far as these intrusions are legally authorised, they are outside the direct responsibility and control of both clients and practitioners alike.

Good practice safeguards against electronic surveillance by national security services include: keeping informed about the implications of such surveillance for any work being undertaken and exercising rights as a citizen to try to influence public policy and the law.

5 Responding to any breach of security or privacy

Practitioners are committed to following the principle of candour whenever a breach of security or privacy arises that could impact on clients. The *Ethical Framework for the Counselling Professions* states:

We will ensure candour by promptly informing our clients of anything important that has gone wrong in our work together, and:

a. *take immediate action to prevent or limit any harm*

b. *repair any harm caused, so far as possible*

c. *offer an apology when this is appropriate*

d. *notify and discuss with our supervisor and/or manager what has occurred*

e. *investigate and take action to avoid whatever has gone wrong being repeated* (Good Practice, point 52).

For further guidance consult the Information Commissioner's Office (ICO) *Guidance on Data Breach Management*. See https://ico.org.uk for more information.

6 Working with vulnerable clients and arrangements for emergencies

When working with clients who are likely to be vulnerable because of their psychological state or social isolation, it is good practice to provide an assessment of their suitability for the services being provided that includes their suitability for working online.

Careful consideration ought to be given to how the practitioner will respond to clients who become so distressed or disturbed that they require additional services or support from healthcare providers or their social network. Good practice requires that practitioners are clear from the outset of working with clients about the boundaries between what is provided by their service directly, how any additional support will be sought in emergency situations by the practitioner, and what depends on clients acting on their own initiative. Online resources or guidance may be provided to assist clients in finding appropriate emergency services, especially where clients are communicating from a distance or it is inappropriate or impractical for the practitioner to seek additional services on behalf of their clients.

Care needs to be taken in communicating to clients what assistance can be offered from a distance in situations where the client becomes vulnerable or distressed or requires urgent support outside the scope of the service being offered. It is good practice to have discussed with clients how they might be assisted before such a situation arises. Assistance outside sessions might be sought from other services including online services, friends or family. Where appropriate, potential additional sources of assistance can be suggested in information about the service or in the contract with the client (see Point 10 below).

7 Legal requirements for working in the UK and Europe

Anyone working online for any aspect of their work needs to take account of the relevant law concerning data protection. The General Data Protection Regulation and the Data Protection Act 2018 set out the legal requirements for anyone who processes data about people in the UK.

The legislation aims to protect the privacy of people and to ensure that people, about whom information has been collected, can check the accuracy of that information. The main implications for the counselling professions include:

- an obligation to register with the Information Commissioner's Office – see https://ico.org.uk/for-organisations/data-protection-fee/self-assessment/y

- the rights of data subjects to access any electronic records held about them – see https://ico.org.uk/media/for-organisations/documents/2259722/subject-access-code-of-practice.pdf

- the necessity of obtaining any client's explicit consent to keeping counselling or closely related records, as these will typically contain 'sensitive personal data'– see *Good Practice in Action 105 The General Data Protection Regulation* (GDPR) and the Information Commissioner's website https://ico.org.uk for more information

- any records should be adequate, relevant and limited to what is necessary for the type of service being provided, and that comply with the applicable data protection requirements. They should be kept up to date; and, not kept for any longer than necessary (i.e. consistent with the client's consent and the purpose for which clients agreed to the records being kept)

- the privacy and confidentiality of any records ought to be protected by adequate physical and electronic security measures – see: https://ico.org.uk/for-organisations/it-security-top-tips

- personal data may not be transferred outside the European Economic Area (EU, Iceland, Liechtenstein and Norway) unless authorised by client consent.

In addition, the law concerning contracts, civil wrongs and crime applies to working online in similar ways to how it applies to working face to face.

The law continues to change and develop in all areas. Changes to strengthen data protection law in Europe are currently under discussion.

8 Working with clients from other countries

The law differs between countries. When working face to face the applicable law is determined by where the work takes place.

When working online it is possible for the practitioner and client to be located in different legal systems and subject to different laws. This creates uncertainty about which legal system applies. One way of reducing the uncertainty is to explicitly state in the contract that the work is being undertaken in accordance with the laws of the practitioner's own country and any disputes will be subject to that country's law. This reduces the degree of uncertainty but does not eliminate it all together. Any contractual disputes would usually be considered in the legal system that applies to the practitioner, provided that this has been included in the contract between practitioner and client. However, any allegations of civil wrongs or crime by the practitioner could still be considered in the legal system that applies to the client's location.

Good practice when working with clients from other countries is to establish their location and to be familiar with the legal requirements that might apply to the work, particularly with regard to civil wrongs including negligence and breach of confidentiality or privacy. Similarly, it is wise to be familiar with any major differences in criminal law. For example, the law in some countries and most states in the USA restricts the right to practise as a counsellor or psychologist. The practitioner would have to meet the local professional requirements to be legally compliant. The protection of the title 'psychotherapist' is more variable but may be restricted to medically qualified practitioners in some countries. Offering services as counsellor, psychologist or psychotherapist in these locations without the appropriate licence or legal authorisation may be a civil wrong and/or criminal offence.

9 Online social forums for clients

There are many successful online social forums that provide clients and people with similar experiences to interact anonymously to break down isolation and share experiences.

Running such sites should not be entered into lightly. They require adequate electronic security, technological support and some degree of monitoring to avoid harmful or disruptive behaviour by some participants. It is considered good practice to have clear ground rules for use of the site, a method for participants to report any concerns – especially about harassment, bullying or sexually inappropriate behaviour and a process for warning or excluding participants who contravene site rules.

As such sites usually run 24/7 they require a team of people and adequate financial resources to sustain their work to an adequate standard.

10 Online information and interactive tools

Online services to clients can be enhanced by providing supplementary information, questionnaires and activities on the host website. Good practice in providing this material includes:

- ease of reading and clarity of communication

- ensuring that readers can assess how recently material has been reviewed and updated by including the date when an item was posted or last updated/reviewed

- acknowledgement of sources and observing copyright

- being clear about materials that are available free of charge and when charges may be incurred

- openly declaring any sponsorship or ownership of the site

- providing contact details for users to contact the site organiser.

11 Insurance

Insurance policies for professional liability vary in whether they cover online or digital working with clients or restrict online work to particular countries. Like any form of insurance, it is important for practitioners to make sure that they have the right type of insurance for the service being provided. If in doubt, ask your insurer.

12 Supervision and training

It is considered ethically desirable to receive at least some elements of regular supervision by the same method of communication that is used with clients, in order to gain direct experience of the strengths and limitations of the chosen way of working.

Changing the method of communication with clients introduces new challenges and opportunities that can be greatly assisted by appropriate training. Good practice requires that anyone making significant differences in their practice should give careful consideration to what will be involved and have taken adequate steps to be competent in the new ways of working before offering services to clients.

13 Personal use of social media by practitioners

Boundaries between your personal and professional activities are as important online as they are working face to face.

It is recommended that practitioners maintain a clear distinction between their personal and professional online presence. All professional enquiries and contacts are best directed to professional sites. Care and consistency are required in how encounters are managed with clients on personal sites in order to ensure that appropriate personal and professional boundaries are maintained.

Practitioners will want to consider carefully how they respond to 'friend' requests on social media. It is best practice to be clear about how such contacts will be managed from the start of the relationship.

Social media sites cannot guarantee any level of confidentiality or privacy and cannot fully remove material retrospectively. There may also be issues of intellectual property, copyright and legal ownership of the material posted.

Good practice suggests that practitioners exercise their rights to use social media for personal communications and relationships online in ways that will neither compromise the work with their clients nor bring the profession into disrepute.

Bringing the profession into disrepute would not usually include a practitioner's use of social media for a lawful personal matter, even if the use might be considered controversial or in pursuit of a minority interest. Best practice in such circumstances is to establish and maintain clear boundaries between personal and professional communications so far as is practicable.

14 Professional vigilance

New technology is opening up life-changing opportunities for so many people. It has made the counselling professions accessible to people who would not or could not use face-to-face services. However, these considerable advantages are also accompanied by new risks. The technology that makes these developments possible is constantly changing. It takes considerable professional vigilance, both individually and as a profession, to keep up to date in order to ensure that the benefits outweigh the risks.

15 Useful resources

Key texts

Anthony, K., Merz Nagel, D. (2010) *Therapy Online [a practical guide]*. London: Sage

Evans, J. (2008) *Online Counselling and Guidance: A Practical Resource for Trainees and Practitioners.* London: Sage.

Jones, G., Stokes, A. (2008) *Online Counselling.* Houndsmills: Palgrave Macmillan.

Weitz, P. (ed.) (2014) *Psychotherapy 2.0.* London: Karnac Books.

16 Guidance on closely related roles

British Psychological Society. *Supplementary guidance on the use of social media* (Accessed October 2015) www.bps.org.uk

General Medical Council (2013) *Doctors use of social media* www.gmc-uk.org

Nursing and Midwifery Council (2015) *Guidance on using social media responsibly* www.nmc.org.uk

17 Online networks and sources of information

Information Commissioner's Office: www.ico.org.uk

International Society for Mental Health Online:

www.ismho.org