www.ACTO-org.uk
info@acto-org.uk

# ACTO Guidance on Security and Privacy for Therapists Providing Online Therapy During the COVID-19 Crisis

ACTO acknowledges that in the current climate, many practitioners and services have only been able to continue to provide a service to clients, by working online. Quite properly, issues of security and privacy have become more widely highlighted, creating anxiety in therapists and supervisors about being able to make the right choice for their practice.

We offer this guidance to enable practitioners, managers – and clients – to understand some of the major issues which have arisen recently.

This is an active document; the guidance provided below is not exhaustive. – it will be updated as appropriate and will be date-stamped accordingly.

N.B. This **guidance does not take the place of formal training** and **does not enable a therapist to state that they are qualified to provide therapy online.**

We recommend that search online regularly for updates on software. In particular we recommend that you read the

- National Cyber Security Centre' Guidance: ***Video conferencing services: using them securely*** which was issued on 21st April 2020.
- Information Commissioner's Office Blog: ***Video conferencing: what to watch out for*** which was issued on 15th April 2020.

## Summary

- Therapists are required by the ICO to have "comprehensive but proportionate governance measures" and "a level of security that is 'appropriate' to the risks presented by your processing". We are required to give high priority to security and privacy – but clearly, we cannot all have 'military grade' security. In addition, our ethical frameworks require us to work within the requirements of privacy and confidentiality, and the current emergency does not change that requirement.
- **At this time, ACTO is unable to recommend any specific online platforms as being totally secure, but advises that therapists explore platforms that follow GDPR compliance.** Things can change very quickly in the online world.



ACTO is the trading name Association for Counselling and Therapy Online Ltd; Registered address: 19B Front Street, Sacriston, County Durham, DH7 6JS United Kingdom. Registered in England; Company No. 10620417; Although our members may not all be resident within England and Wales any ACTO contract, and the work to which it relates, are subject to the jurisdiction of the laws of England & Wales.

- There is a range of platforms – from those originally designed for social use, to those with privacy by design built in. Therapists need to keep themselves informed and updated on the availability of platforms and the choices available to them.
- No platform is 100% secure. What we do as therapists and how we use platforms and their features will ensure that privacy and security are retained for therapeutic work.
- This guidance aims to help therapists protect their client's safety and security as far as is possible in the context of their practice and so to demonstrate the principle of due diligence.
- ACTO recommends therapists make the known risks at any given time explicit to their clients and that this is documented within paperwork.

## What is expected of therapists?

The ICO says this about security and privacy:

"***What level of security is required?***
*The GDPR does not define the security measures that you should have in place. It requires you to have a level of security that is 'appropriate' to the risks presented by your processing. You need to consider this in relation to the state of the art and costs of implementation, as well as the nature, scope, context and purpose of your processing.*

*This reflects both the GDPR's risk-based approach, and that there is no 'one size fits all' solution to information security. It means that what's 'appropriate' for you will depend on your own circumstances, the processing you're doing, and the risks it presents to your organisation.*"

***https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/*** [Last accessed 23/04/2020]

And:

"*You are expected to put into place comprehensive but proportionate governance measures. Good practice tools that the ICO has championed for a long time such as privacy impact assessments and privacy by design are legally required in certain circumstances that pose a risk to the rights and freedoms of individuals.*

*Ultimately, these measures should minimise the risk of breaches and uphold the protection of personal data. Practically, this is likely to mean more policies and procedures for organisations, although many will already have good governance measures in place.*"

***https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/accountability-and-governance/*** [Last accessed 23/04/2020]

## A therapist's understanding versus business technology terminology?

As therapists we have well-developed notions of what 'privacy' and 'security' are. However, **technology companies use them with different emphases and meanings,** which can trip us up. So here we explain how these terms are **used by technology companies,** specifically as they impinge on therapeutic practice online.

## *What is security?*

Security has a number of aspects:

- First, like a security door and locks on a house, IT software needs to balance accessibility to those with a legitimate reason to use it with preventing non-permitted access. With online video meetings, only those invited should be able to gain access. This does not have to be preventing only illegal or malicious access, but includes inadvertent stumbling into a meeting. **Security in this sense bolsters privacy but is not equivalent.**
- Second, we need to play our part and not "leave the keys in the front door"… or leave the therapy room door open. We need to understand which features of the software enable us to maintain a private and safe space. Therapists have the power to make very simple changes to how they use software to make it far more secure. If you do not understand how the software works, it is best to choose not to use it.
- Third, continuing the house metaphor, security is like ensuring that the building is robust and not going to fall down. Software needs to run reliably without crashing too often. It also needs to ensure it has the capacity to run with a lot of users. Video conferencing companies recently have had to increase their capacity with large increases in people working from home. Continuity of service is an important part of security.

## *What is privacy?*

- Privacy means ensuring that any platform or company providing a service which handles personal data (ours, or our clients), keeps it private and doesn't share it with others.
- Security as discussed above protects against exposing personal information unintentionally through poor software design choices. **However, companies providing online services require access to a lot of information to function some of which can be used to identify an individual person.**
- This information **(or data)** is carefully protected by legal codes which vary from country to country.
- In the UK and EU the relevant legislation is the **GDPR.** Each company operating in the UK has to **state explicitly how it meets the requirements including** why they collect the data and what they lawfully do with it.
- Anything **anyone does** with data is known as **'processing'** and what **companies do or intend to do is articulated by a privacy statement.**
  The problem is that these are rarely written in clear English and this obscurity can often afford the companies leeway to use the data in ways beyond those needed for the functioning of their service.
- **Sometimes the companies themselves do not appreciate fully what is being done with personal data. A very common scenario is that data is shared with marketers** – the income from this enables the companies to offer their software **for free**. This could be a significant problem for therapeutic work. **Visiting a therapist's website** might indicate that someone is considering therapy. People might expect this to remain private, but **tracking software can expose this to others, which seems inimical to privacy.**
- We would almost never do that in face-to-face work**, but we may be doing that inadvertently when using software to provide therapeutic services or having a website** with common 'analytics'.

## *What is encryption?*

- Encryption is like **using a very strong password**. Without possessing the password or 'key' the data is scrambled and so meaningless. Like a password if it falls into unintended hands, full access to the data protected by it would be gained. You can encrypt data when it is on your own computer or other local storage e.g. a USB drive.
- You can also encrypt data as it is communicated across the internet so that interception and accessing during transmission is virtually impossible.

- **It is more secure to do both of these**. Many services encrypt data when it is transferred across the internet, but retain the ability to view the material as it passes through their service.
- **There will usually be policies in place discussing access, but a better solution is for the organisation to not know the key to decrypt the data**: this is described as 'zero knowledge'.
- This carries a risk – if you forget the key you will not be able to access your data. With video conferencing all you are likely to want to ensure is that the data is only accessible to you and your clients and that it disappears after your session has ended. So, you will need to establish that it is encrypted during transmission and not saved once you have finished.

## General guidance for therapists

- **You (or a service you work for) must Register with the ICO**. We are all data controllers or processors by virtue of our practice.
- Check that **your insurance provider covers the practice of online therapy. For instance,** you might not intend to work internationally but you may find your clients are not always in the UK.
- Check if you need **separate insurance covering cyber-attacks e.g. 'ransomware'.**
- **Communication via video** is the closest online medium to providing face-to-face therapy. In the absence of a suitable qualification and experience we recommend that therapists work in video with their already known clients/patients **only if they can provide basic security/privacy measures and where appropriate supervision is in place.** This may need to take into account the needs of newly qualified or inexperienced supervisees in working via technology.
- Consider using headphones for all sessions (if possible: hearing aids might make this hard) for both sound quality and privacy reasons (i.e. the client not being overheard inadvertently).
- Work from a comfortable private space where you cannot be overheard – a door lock might be appropriate.
- If you use a shared computer for clinical work, ensure access to your files and programmes etc is protected by having a **separate user account with a strong and private password.**
- Computer – ensure you have a **good firewall and anti-virus/anti-malware software installed** (**free** software is often **less** effective than paid software).
- Make sure you do not sit with light immediately to the side or behind you as this makes it difficult for the client to see you well.

### *Before each session*

- Internet – with households sharing one connection to the internet, it is best to reduce the demands placed upon it as much as possible by **closing any programmes** not needed while you work. You may have to negotiate exclusive access with other **members of your household** if your connection is particularly slow. Sometimes this can be because of Wi-Fi demands so, if possible, use **an ethernet cable** to ensure a direct link to your internet router.
- **Shut down** any search engines.
- Ensure that **all active programmes** on your computer are shut down. For instance, **stop any software such as Dropbox synchronising** in the background as these will definitely slow your computer down.
- **Turn off all listening devices** e.g. "Alexa", "Siri" and similar apps on mobiles and smart watches.

## *Emails – sending session information and other administrative details*

- General email accounts are not private – they are **similar to sending a post card** rather than a sealed and tracked letter.
- There are ways to reduce the risks here: you might want to discuss these with your clients. **First, having a separate email account for professional work** is helpful for maintaining therapeutic boundaries.
- **Second**, you can send a password-protected document as an attachment to your client. This is similar to sending a sealed letter. This might be the most protection your client can tolerate.
- **ACTO recommends using encrypted email accounts** such as Protonmail, Hushmail, SecureMail, Frama.
- **Full** encryption means that the email content **can only be viewed by the intended recipient** as long as both parties are using shared encryption: the easiest way to ensure this is to be both **using the same secure email service**.
- With all of the solutions the fact that you (a therapist) are communicating with someone could potentially be exposed**, but only fully encrypted email protects the content robustly.**
- **Emails are best limited to sending factual information**. It can be tempting to get drawn into a therapeutic communication. If this happens, it is advisable to acknowledge what the client/patient has informed you of and reassure them that this can be explored further during the next session.
- It is advisable that the signature of your email repeats the message that **you do not provide crisis support and provide links to appropriate organisations that do.**

## *Other forms of textual communication*

- Texting a client on a mobile phone is relatively secure but **not suitable for therapy** as people have names of clients on their phone and it can be too easy to text the wrong client – though see next section on using client codes.
- **Using a separate and more secure encrypted texting application** on your phone that would keep the content of the messages away from your mobile phone operator's archive. They are required to keep regular text messages for up to a year by law. Most clinical information would not be of interest to legal officers, but again it is preferable to design into your practice avoiding the potential for it to happen.
- **Having a separate phone for client work** will ensure clients do not have access to your personal phone number. This also helps to ensure boundaries such as times of therapist availability and can be locked away outside of your working hours.

## *Client/patient identity*

- For your information **assign each client/patient an individual abbreviation** that does not reveal their full name or sensitive details. This is known as 'pseudonymisation'.
- **Do NOT put links to online therapy sessions in an online calendar**. That would add another potential leak of the data.
- Safe practice would be ensured through **sending details of sessions and links within an encrypted email NOT via text or unencrypted email.**

### *Communication platforms and privacy*

- At the present moment we recommend that, whatever platform you chose to use, you need to **inform your client/patient** that you are **unable to ensure** the platform will not share any sensitive information that the platform is able to access.
- ACTO recommends that you check online whether the platform or software you are planning to use is data-mined by its owners.
- It is possible that their **sensitive information might be shared with companies and that might impact on them now or later** e.g. insurance or other financial companies. As data controller y**ou need to inform them of their rights as a data subject as laid out by ICO** ***https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/***

### *Risk management and safeguarding*

- When working online you will **need to think at all times about risk management and safeguarding,** both are more difficult at a distance and will need careful completion and documenting. For example, using live chat might be a danger if someone is in a relationship where a partner is monitoring their phone or computer. Equally you'll need to think about how to manage such matters when the client is far away from you geographically. These examples are illustrative not exhaustive.
- Check that you have knowledge of **the exact location** of your client before the beginning of any session along with possession of alternative contacts in case of emergencies. For any safeguarding or risk management involving the authorities, especially cross-border, ensure that you have full name, address, phone numbers, email and date of birth. This will be necessary for Interpol should you need to risk manage with a client who is cross-border.

## Conclusion

In conclusion we hope that this guidance has helped you to appreciate some of the issues to consider when moving your practice online at this difficult time. We have tried to demonstrate the continuity in practice of prioritising the privacy and security of the therapeutic frame, albeit in a different technical context. It's a fine balance between being pragmatic and living within the required security and privacy governance, our own limits of competence and our ethical frameworks.

We are trusted with the most intimate details of our clients' lives: we already treat this with the utmost respect. We hope that sharing these ideas born from our collective experience helps you to feel more confident honouring that respect in a new technological context.

We would warmly welcome members sending contributions to this subject. These should be sent to ***info@ACTO-org.uk***.

*The Board of Directors has put together these* ***Governance and Good Guidance Notes*** *in good faith for the benefit of ACTO members and the general public whom we serve. It has been prepared as honestly as it can been with the knowledge available. Nevertheless, the Board of Directors declines all responsibility for any inaccuracies and would encourage each reader to go and carry out their own research on this subject.*