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

ACTO BOARD OF DIRECTORS

GOVERNANCE & GOOD GUIDANCE NOTES FOR MEMBERS

Subject: **Is Skype a suitable tool for online therapy?**

Issue Date: **14 August 2017**

Last Update: **09 November 2018**

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 to their own research on this subject.*

Q "Skype came up in conversation in my NHS job in context of using it for clinical supervision.... I suggested it wasn't secure enough but the service lead told me they've purchased business skype and that it is."

Well what's the truth about Skype and Skype for Business?

In 2013, Pip Weitz was prepared her book Psychotherapy 2.0 (Weitz, 2014b) undertook some research into whether Skype was suitable for therapeutic purposes. She approached Microsoft, the owners of Skype, and they confirmed that Skype was not suitable to be used for therapeutic purposes. She also documented her conversation with the Information Commissioner's Office, which confirmed the same. Her findings and various writing on this subject has been available on www.pwtraining.com ever since. (Weitz, 2014a). Please see below this text for the references to various links.

Three years on, we were asked the question above and thought we should explore the Skype question again, and broaden this issue out a bit further. Bond (2017) in his review of Weitz's book (2014) book said: "*the reservations expressed about Skype could also apply to other platforms, to some degree*". As a Board of Directors we couldn't agree more and the comments we include below may well apply to other software.

And now we have GDPR. Does this change anything?

= = =

In 2016 Dr Carole Francis-Smith (2016b) reviewed of both Skype and Skype for Business and summarised very fairly its strengths and weaknesses.

The two big issues now, in 2018, are:

1) **We use the word Skype generically** …… the difference between Hoovers (another word used generically) is that most if not all vacuum cleaners more or less do the same job, there is not an overtone or undertone to the use of the word "Hoover". This is not the case with Skype. When we say "Let's Skype" it means let's communicate online via video …… the problem is that the word Skype used in this context subliminally endorses the use of Skype. So just a little plea, please do not to use the word Skype generally when we're speaking in a therapeutic context as it provides a mixed message about whether it's OK or not. Let's just talk about working via video, or video-conferencing. It may be a bit more long-winded but it stops the misunderstanding that creeps in by using the "S" word!

2) **GDPR has changed everything.** We simply cannot continue to ignore the obvious. For example, as we will see in much more details below ibn item 2, it is simply not acceptable for clients to see when you, their therapist, is or is not online, and vice versa, it is not OK for you to see when a client is or is not online. The issue is not limited to Skype, VSee has the same dependence on contacts lists.

   What is great and helpful amongst families and friends is simply intolerable for psychotherapists working professionally.

Everyone misguidedly talks about how Skype is not encrypted. This is a myth. It is encrypted. This is a good point. There are many good points about Skype and many millions of people use it for personal purposes without any problems. A similar example you might make a comparison is between an accountant using a home accounting package for his work rather than using Xero or another professional accounting package.

But Skype is generally not considered very secure, as you can read up on at this website: https://www.comparitech.com/blog/information-security/is-skype-safe-and-secure-what-are-the-alternatives/

GDPR now requires us all to have a private policy and implement it.

- Essentially GDPR is about giving the individual control over their private data.
- Consent can no longer be taken for granted, it must be active rather than passive.
- Data controllers are required to demonstrate accountability, for example in contracting arrangements and data sharing.

In other words we can't just go on as before. Please just hold thet thoughts about GDPR, privacy and an individuals' control over their over data as we explore further the Skype issue.

We have already established that Skype is encrypted (many people do not realise this, but both Slype and Skype for Business are encrypted). This is a good thing.

Issue 1 Advertising

The first issue, relates specifically to Skype and is that Microsoft raid the Skype accounts to sell your data. We're all used to seeing the ads flying around our skype screens. So that's one issue with Skype. From a GDPR point of view we did not ask for these ads.

Skype for Business does not appear to attract advertising (remember I don't use this) and their Microsoft Online Services Privacy Statement which is the Skype for Business version of their Privacy and Cookies Information confirms they won't share your data.

Issue 2 Contacts Lists

The second issue is the contacts list. This is the big issue that completely fails GDPR privacy requirements. VSee has this problem, Skype has this problem, and other platforms may have this problem. **Zoom does not have this problem.**

That's one of the reasons we like Zoom. Zoom has no contacts list and you simply send your client / patient a link each time.

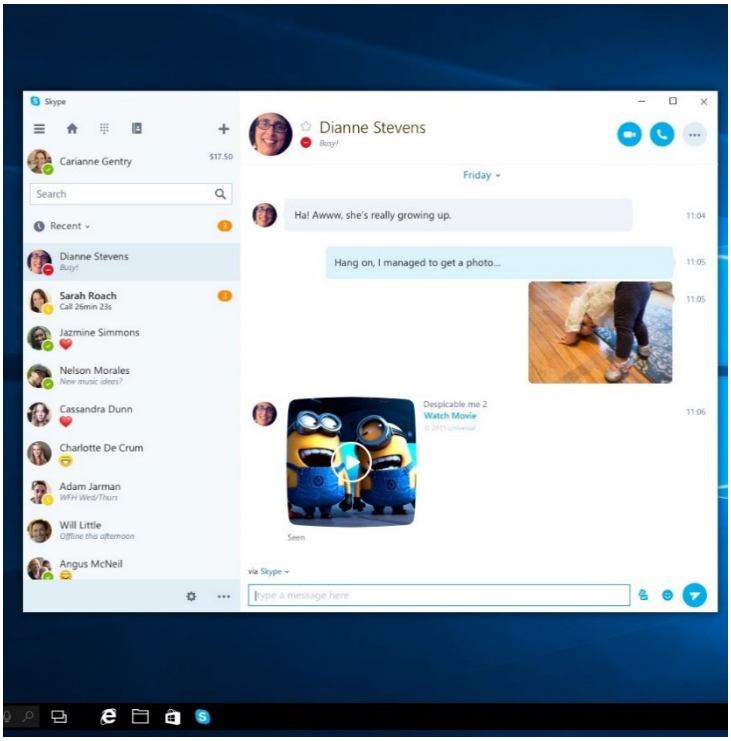

Figure 1 Skype contacts showing clients online at any time

Skype has a very nasty habit of turning itself on just when you don't want it to and unless you hard quit Skype (by for example right clicking the icon on the bottom bar and selecting quit Skype), it will try and resurface.

If your Skype is running in the background it is possible, and it does happen, that your address book could be showing all your contacts INCLUDING YOUR CLIENTS and whether they are online or not (see Figure 1). Please imagine the people showing in Figure 1 are your clients – you'd go into meltdown if these kept appearing on your screen! This is definitely a breach of the data protection regulations / GDPR because a colleague could suddenly come and look over your shoulder whilst you were deep in thought or when you were screen sharing.

At all times my Skype address book shows me who is online …. Whether it's a client or friend. This is completely unacceptable for clients, whilst it's extremely useful and practical for friends. So yet another data protection breach.

GDPR requires us to think of the privacy of our clients and colleagues AT ALL TIMES. So often being human is our biggest weakness, and all that may be required is a better management of our computers, it is an example of sloppiness by the data controller (you as therapists in this context) by leaving the contacts open on the screen and it's our responsibility to manage this issue. The easiest way to manage it is not to use Skype or VSee or similar. And that is easy now as there are other systems in place that comply without major cost. The one we find fits the bill the best is www.zoom.us. Zoom does have the capacity to have a contacts' list but you do not need to use it. Best practice is to just send the link or Meeting ID (a series of numbers) to the client for the session and once the session is over any trace of it has gone.

You may say this is a little zealous, but how many of us have worked with clients who have been stalked or tracked on their computers by a jealous partner? Whilst a very clever stalker may crack any software, selecting a good platform as a basis for our online work is a duty of care to our clients and will go a long way towards their protection.

Issue 3
A paper trail

There is also the issue of the paper trail left in live chat in Skype (see Figure 2). In Skype the live chat function is what provides the risk as the texts are stored online and available well after the "session" (for 30 days) and not password protected or security protected in any way. Yet another breach. On Skype for Business in live chat the issue still exists, albeit in a slightly different way as you can have open, closed or secret chat rooms but the text is retained unless deleted meaning the same breach issue occurs and the text might available, though perhaps it is less of a breach as it is more hidden. The live chat function on either Skype or Skype for Business does not provide a suitable level of security for the therapeutic use as the text is still available at a later date and could be misused (think about for example a jealous partner using tracking software).

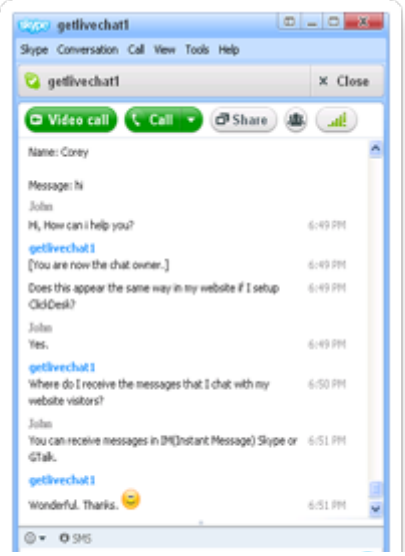

Figure 2 Example of Live chat

Microsoft is quite open about the way it accesses and use your data. Here's what Microsoft (2017) says about its use of data and privacy on Skype for Business in its Terms and Conditions:

"Microsoft collects data to operate effectively and provide you the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, submit a search query to Bing, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN [Microsoft Developer Network] *subscription, sign up for Office 365 or contact us for support. We get some of it by recording how you interact with our products by, for example, using technologies like cookies, and receiving error reports or usage data from software running on your device. We also obtain data from third parties.*

And here's part of what it says under the Skype Terms and Conditions (2017):

"As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or usernames that are part of the communication. [….]

If you use a Microsoft service, such as Outlook.com, to manage contacts, Skype will automatically add the people you know to your Skype contact list. With your permission, Skype will also check your device or other address books from time to time to automatically add your friends as Skype contacts. You can block users if you don't want to receive their communications."

Issue 4
Screen Sharing

One of the most useful tools of video-conferencing is our ability to screen share. However, this could also be your downfall.

Skype screen share: If you screen share with your client (or anyone else for that matter) you can bounce between all the screen you have

open, this could include your Outlook Contacts List, a contract with a client, client notes etc. Using Skype Screen Share allows the user to move seamlessly between all the Windows you have open. Another GDPR failure for us as therapists.

Zoom screen share: The default Zoom screen share is that when you select screen sharing you have to select the screen you want to share with the other person ……. This reduces dramatically potential data privacy breaches. There is one caveat to this – a web browser is seen as one screen share …. But you can have multiple pages open in that screen browser, e.g. your bank account, mailing list, etc and if youi move between these pages there is a danger that someone may see a page they should not see. In this instance we would advise you always to close down confidential pages between screen sharing a web browser such as Chrome.

Conclusion

These are extremely scary statements in terms of the privacy that we are required by law to provide as data controllers to our clients and patients. The examples we include here are not exhaustive but are examples of what might be really helpful for us as family and friends is not at all suitable for therapeutic purposes. It's a leaky as a sieve!

We hope we have given a comprehensive explanation (though not exhaustive) of why we are therapists might well do better to steer clear of both Skype, just as the accountant wouldn't use the home accounts package for his professional work. We will be very happy to be corrected if you feel we are wrong.

The one thing we would ask if you do engage is a discussion about the use of Skype is that you are respectful about it so that we as a profession can grow the body of information around working safely online for both ourselves and our clients.

We end with Tim Bond's (2017) recent statement on the subject:

"*Ideally, it is better to use more appropriate platforms for psychotherapy, where these are available and acceptable to clients*".

References

Bond, T. (2017). *BookREVIEW: Psychotherapy 2.0: Where Psychotherapy and Technology Meet.* http://www.contemporarypsychotherapy.org/volume-9-no-1-summer-2017/bookreview-psychotherapy-2-0-where-psychotherapy-and-technology-meet/ . [Last accessed 12 August 2017]

Francis-Smith, C. (2016 – 2017a). *Software reviews.* https://privatepracticehub.co.uk/onlinetherapyhub/category/software-reviews. [Last accessed 12 August 2017]

Francis-Smith, C. (2016b). *Review of Skype & Skype for Business. 31st May 2016.* https://privatepracticehub.co.uk/onlinetherapyhub/blog/skype-skype-for-business [Last accessed 12 August 2017]

Information Commissioner's Officer. (2017) The guide to data protection. 7th July 2017. https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/ [Last accessed 12 August 2017]

Microsoft. (2017) Microsoft Private Statement. June 2017. https://privacy.microsoft.com/en-gb/privacystatement [Last accessed 14th August 2017]

Weitz, P. (2014a) *A Summary of Philippa Weitz's conversation with the ICO summer 2014 - the Skype issue*. https://www.pwtraining.com/resources/articles-for-working-online/security-confidentiality-online/ . [Last accessed 12 August 2017]

Weitz, P. (Ed.). (2014b). *Psychotherapy 2.0: Where Psychotherapy and Technology Meet*. London: Karnac.

Weitz, P. (2014c). *The role of confidentiality and security for working online – our responsibilities as psychotherapists & counsellors - a position paper*. https://www.pwtraining.com/resources/articles-for-working-online/security-confidentiality-online/ [Last accessed 12 August 2017]

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