Cyberwork

Keylogging – who's watching you?

Kate Anthony

The importance of client confidentiality and privacy are a given in our profession. Yet keylogging, which is a simple and often used technique in the workplace, constitutes a huge threat to confidentiality, and many practitioners are unaware of this.

Keylogging is the installation of a piece of software (or sometimes built-in hardware) that simply records every keystroke you make, usually without your knowledge. The most nefarious use of a keylogger is for cybercrime, recording passwords and account details to take identities and bank details. However, it also has many positive uses such as its use in writing process research; anti-crime measures taken by the police and other authorities; and ensuring your children's computer use is not harming them.

Within the workplace, employers often use keylogging to ensure that employees aren't wasting company time on personal projects, or using company hardware to look at pornography, participate in online gambling or other unacceptable practices. This is both legal and widely regarded as acceptable within the specific context of one's place of work.

'If you are a counsellor in the workplace, communicating with clients via technology, whether for direct therapeutic work or simply for administration purposes such as setting appointments, you have a duty to your clients to ensure you know who has potential access to their data and for what purposes, from your line manager to your IT department'

But what of those of us employed to use technologically mediated communication methods to work with clients? Our remit as counsellors and therapists under the umbrella of the BACP *Ethical Framework* remains the same: 'The professional management of confidentiality concerns the protection of personally identifiable and sensitive information from unauthorised disclosure.' And yet, the usually covert practice of keylogging by employers is often overlooked as an example of an 'unauthorised disclosure'. On the other side of this is the client who is unaware of keylogging, potentially allowing his or her employers access to what could be work-related, sensitive and private material.

One of the first dilemmas my students face in the clinical practice section of training is the scenario of the client who wants to use a work computer to receive online therapy, so that she can keep the process of seeking help for depression and anxiety, from her husband. There is a fine line between allowing the client autonomy in deciding the best method of receiving online help and where they access it, and the need to educate them in doing so with respect to their privacy. This can range from advising them, for example, not to print the content of therapeutic sessions and then leave it on the kitchen table; not to use a public computer service, such as a library, where their actions may be seen by others; and advising them of the need to check who has access to their computer data. By making this topic one of the first dilemmas within our ongoing case study in the training, we instil an ethic that goes further than just having the desire to use a device to communicate therapeutically with clients electronically and learning how to do so: we ensure that issues of confidentiality and privacy require vigilance and are assessed on a case-by-case basis in the practitioner's future work.

If you are a counsellor in the workplace communicating with clients via technology, whether for direct therapeutic work or simply for administration purposes such as setting appointments, you have a duty to your clients to ensure you know who has potential access to their data and for what purposes, from your line manager to your IT department. If your workplace uses keylogging, it is usually for quite reasonable purposes such as monitoring employee output and combating cybercrime rather than catching you out at the occasional foray into eBay or Facebook during your lunch hour.

To find out more about employer access in the workplace, first check your company's privacy policy regarding employee computer use, if it has one. This may detail the exact circumstances under which device monitoring is used. You could also ask the IT department or your employer directly about this, and discuss with them the importance of keeping your clients' confidential material exactly that – confidential. Finally, if your company's policy on monitoring the use of their electronic property is set in stone, ensure your informed consent documentation with clients includes this information. It is only with appropriate knowledge of such elements of the use of technology that we can move towards secure, confidential, private therapeutic communication as we knew it before the invention of the internet.

Dr Kate Anthony, FBACP, has trained practitioners and organisations worldwide in online therapy and related fields and is a Fellow of BACP. She is co-founder of the Online Therapy Institute and Managing Editor of *TILT* Magazine (Therapeutic Innovations in Light of Technology).
www.onlinetherapyinstitute.com