The Bar Council

Remaining compliant and IT secure when working from home

Purpose:	To provide assistance to barristers on GDPR and IT security matters when working from home
Scope of application:	All practising criminal barristers
Issued by:	The IT Panel
First issued:	March 2020
Last reviewed:	February 2022
Status and effect:	**Please see the notice at end of this document. This is not "guidance" for the purposes of the BSB Handbook I6.4.**

Introduction

1. The Bar Council is aware that following the coronavirus outbreak working from home, or away from Chambers, is now increasingly common; with remote CVP hearings being regularly used. The following is advice on how to remain GDPR compliant and how to keep your data and devices secure while doing so. A list of links to more detailed guidance is set out at the bottom of each section.

Home working and IT Security

2. Firstly, which computer are you using at home to work? If you brought home your laptop from chambers (possibly even lugged home your desktop?) then it is, of course, already encrypted (isn't it? Make sure …). If you have brought your work computer home, make sure it is physically secure as well - (lock it away when not in use, if possible). Definitely log out and turn it off when not using it.

If you're using your home computer, which isn't usually used for work, think about the following:

- make sure it's encrypted if at all possible: don't forget that a silk was sanctioned by the ICO because their laptop was stolen from home: it contained highly sensitive personal data relating to clients, but was not encrypted. If your computer is not capable of appropriate encryption, think about replacing it or using an external hard disk capable of being encrypted. The ICO took the view that the failure to encrypt the laptop meant that the silk had failed to take appropriate steps to secure the confidentiality and security of that data, and that being a victim of theft did not alter that. Whilst there might be an argument that working from home may reduce the chances of theft (as there may be more people around) it remains the case that it may happen and, if you now work on your home computer, it will contain personal data and so needs to be encrypted.

- who else has access to the computer? If it is used by others in the household, you need to set up a separate account to keep your data separate. Your account should also be the only one with administrator access, to make sure that the data is secure – another barrister was fined by the ICO when a family member accidentally uploaded client data to an unsecured cloud server during a software update.

- make sure that the operating system is up to date and that all antivirus (!) and similar security software is up to date, particularly if there are household members who tend to download games and other material which might carry an unexpected payload with it (you do not want to be exposed to key loggers and other such malware).

Regardless of whether it is your work computer or a home computer, make sure that the screen isn't visible to others whilst you are working; make sure you close the computer (if a laptop) or set a screensaver going (with a password!) if you have to leave the computer unattended briefly.

3. Check your backup options: if you rely on chambers' server backups, are you able to connect to the chambers network from home? If not, you will need to make sure you have your own backup provision. If you can access chambers' network from home, make sure you do so and don't simply save material on

your hard drive.

4. Consider the security for remote accessing the Chambers network, or cloud based servers, with two-factor-authentication strongly recommended. Microsoft 365 offers this as standard but it is often not enabled. If, as is recommended, you back-up to the Chambers networks or remote servers ensure that these are secure. At the very least use a "strong" password; check that those in Chambers with "admin logins" is kept to a minimum; and encourage all tenants to keep their logins secure (engage two-factor-authentication and use strong passwords).

   Remote working is extending beyond working from home. Barristers are now commonly attending one court center in person, and remote accessing hearings or conferences held in other locations. When working outside of chambers or your home, consider the security of the Wi-Fi you are accessing. Court and other ".gov" Wi-Fi internet access is generally secure; however, public/open networks which require no passwords are significantly less safe. Maintaining the most recent updates on your virus software will provide some, but not complete, protection when using public Wi-Fi. As an alternative to public Wi-Fi, use a personal Wi-Fi dongle, or if you must use Wi-Fi, use a private link. Consider using trusted VPN software.

5. While you are thinking about IT security don't forget the physical security of your devices and files, and of access to them in your home: if you bring paper files home, make sure that these are not left lying around and that they are locked away when not being used. Consider getting a household alarm if you don't already have one - to secure the room in which you store files, at least.

Useful links to Bar Council guidance:

- Advice for those travelling
- Back up work on your PC
- Information Security
- GDPR: Frequently Asked Questions
- Mobile Device Security

Decontaminate your IT

6. If you have brought your IT devices from work (or used your smartphone

without washing your hands) you may want to consider physically decontaminating them as well. You should follow any guidance from the manufacturer about the sensible methods to use. Be aware, that not all devices are waterproof! You will almost certainly want to switch it off before attempting any cleaning. Use gentle non-abrasive cloths. Microfibre glasses cloths are useful to avoid damage to screens and coatings. Low concentrations of alcohol or soap may be suitable, but check before you use them. Disinfectant wipes may also be suitable.

Remote Hearings, and Telephone & Video conferencing

7. CVP links are often published in different parts of the Digital Case System depending on the Court arranging the link; with some Courts being more efficient than others. You are often encouraged to publish your contact details (cjsm email address and contact telephone number) as a 'widely shared comment' as early as possible to arrange contact between Court Staff and Counsel covering a hearing. Microsoft Teams is used both in Tribunals and in the Senior Courts. This may require log-in details. Your solicitors will probably have a conferencing app which they favour. Check in advance of any con that it works on your system, and that you can maintain confidentiality when using it.

Useful links to Bar Council guidance:

- Internet Security

Document access/File sharing

8. If you need to get access to large volumes of documents, you will probably need to make sure that your home broadband is up to it. If it is an issue, consider upgrading to a faster option, if that is possible.

   If you are going to use cloud computing to store or share files, make sure you follow the guidance below.

Useful links to Bar Council guidance:

- Cloud Computing

Increased risk from Phishing and other exploits

9. If you are working remotely more than before please be aware of the risk that criminals may seek to exploit this with phishing emails. Be vigilant about any communication which seems "off". Check by direct contact if that is possible.

For more information, please consult the Bar Council Ethics Hub's IT pages here.

Important Notice

This document has been prepared by the Bar Council to assist barristers on matters of information security. **It is not "guidance" for the purposes of the BSB Handbook I6.4, and neither the BSB nor bodies regulating information security nor the Legal Ombudsman is bound by any views or advice expressed in it.** It does not comprise - and cannot be relied on as giving - legal advice. It has been prepared in good faith, but neither the Bar Council nor any of the individuals responsible for or involved in its preparation accept any responsibility or liability for anything done in reliance on it. For fuller information as to the status and effect of this document, please refer to the professional practice and ethics section of the Bar Council's website here.