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 barristers
Issued by:	The IT Panel
First issued:	March 2020
Last reviewed:	May 2023
Status and effect:	**Please see the notice at the 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 UK 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. In November 2011, the ICO sanctioned a silk whose laptop had been stolen from their home. The laptop contained highly sensitive personal data about clients and was not encrypted, meaning in principle it was easier for thieves to have accessed the client confidential data.

- 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.

- Ask yourself, who else has access to the computer? If it is used by others in your household, you should 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. In March 2017, a barrister was fined by the ICO when a family member accidentally uploaded the barrister's 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 security software is up to date, particularly if there are household members who tend to download games and other material which might include unwanted or unexpected data, or 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 and while travelling and make sure you close the computer (if a laptop) or set a screensaver (with a password) if you have to leave the computer unattended briefly.

3. Check your options for backing up your data. 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. Restarting your computer on a daily basis is also encouraged. Leaving your computer in sleep or in hibernation may be more convenient but does not allow for software security updates to be installed. Turning the computer off at the end of the day will allow for updates when the computer is restarted.

4. Implement two-factor or multi-factor authentication (*"2FA"* or *"MFA"*) for remote access of the Chambers network. MFA requires additional corroboration to the entry of a password when accessing the Chambers network. Microsoft 365 offers two-factor authentication as standard but it is often not automatically enabled. Further, 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).

5. Remote working has long since extended beyond working from home. Barristers are now commonly attending one court centre 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 mobile telephone hotspot. If using your mobile telephone as a Wi-Fi router, ensure that your phone is running the latest operating software. Also, if sending emails from an Apple iPhone, be aware of the preference you have selected for *'Include Attachments with Replies'* (Settings – Mail – Composing). Apple changed the default setting so that attachments will not be included within a reply but will be included if the reply includes a new recipient. If you must use a public Wi-Fi, use a private link. Consider using trusted VPN software.

6. While you are thinking about IT security remember 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 or safe 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

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. 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 conference that the relevant technology works on your laptop or desktop, and that you can maintain confidentiality when using it.

Useful links to Bar Council guidance:

- Internet Security

Useful links to Bar Council guidance:

- Cloud Computing

Increased risk from Phishing and other exploits

8. If you are working remotely, please be aware of the risk that criminals may seek to exploit this with phishing emails. Be vigilant about any communication which seem suspicious. Confirm through direct contact if that is possible.

9. Be aware of suspicious emails from solicitors or suppliers. Supply chain cyberattacks are when a vulnerability in a company or individual's cyber defences is exploited to attack another actor to whom they supply services. An SRA report dated, 1st June 2022, highlighted that attacks on third-parties or IT Providers can also affect firms, noting that attacks last year on service providers and a barrister's chambers both spread to multiple solicitors firms.

The Information Security Questionnaire for all centralised services provided by Chambers (or the Questionnaire for short) was devised by a joint Law Society / Bar Council working group in part to reduce the risk of supply chain cyberattacks. Solicitors firms who issue the Questionnaire to chambers will have assessed their vulnerabilities to a similar standard, and confirmation of completion of the Questionnaire can reassure firms that these chambers are not the weak point in the supply chain.

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.