Advice for those travelling

Purpose: To encourage barristers to plan ahead in relation to appropriate IT provision, remote access and hardware encrypted USB drive use when away from Chambers

Scope of application: All practising barristers

Issued by: The Information Technology Panel

Issued on: December 2017

Last reviewed: January 2021

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.**

1. We recommend assessing, minimising and further mitigating risks associated with taking work away or accessing work from afar, particularly when travelling abroad. Barristers should always evaluate whether their proposed use of IT follows best practice in relation to computer security and data security. The primary risk lies beyond any financial loss for replacement of a lost or stolen laptop or mobile device. Your primary concern in planning IT for travel should be the potential impact of the loss or compromise of any professional or confidential information on a device lost or in a computer account accessed by a third party.

2. Professional documents will almost always contain commercial, sensitive and confidential information the loss of which would impact on your professional relationship with a client as well as your reputation. Any loss or compromise may oblige you to notify the Information Commissioner and clients with the attendant professional embarrassment, investigation or even fine. Any material is suitable for misuse: even a corporate address book with details of employees or contact details could be used in a spearhead or targeted phishing attack.

Identify technologies with particular risk

USB storage devices

3. USB storage devices can contain many tens of thousands of files and are particularly easy to misplace given their size. Check that any USB device you use comes from a reputable supplier and manufacturer with integral hardware-based encryption or use reputable software encryption. Preferably choose one certified to the FIPS-140-2 standard. Be aware of the widespread counterfeit USB flash drive capacity scam which would put you at risk of lost or damaged documents by data loss. Even mainstream UK online retailers have allowed counterfeit USB device to be listed and supplied.

4. Consider secure-wiping any partially used USB drive before travelling and re-format before use so that you can be confident that you only place on the drive the specific files you are likely to need whilst you are away. Utilities are available to check the integrity of a USB drive (for an example list of utilities available see https://www.geckoandfly.com/22803/detect-fake-usb-flash-drives-sd-cards-ssd-disk/) For each file or group of files on the drive, consider who are the data subjects, then clarify or confirm that the extent of your existing permission to work on the data in Chambers extends to your placing it on an external USB device (albeit encrypted) and taking it away from Chambers or outside the UK.

5. If you take data with you on a USB device, external drive or mobile phone, you should only plug the device into a computer you can reasonably trust.

6. You should be very sceptical about trusting any computer other than one you fully control and routinely use. Any computer into which you might insert the drive is able to have been in some way compromised before your use of the computer and software could be installed which is controlled by another person or organisation. Such software could compromise the privacy or the integrity of all the files on the drive.

7. What are the implications for you if the entire contents of your USB were available to the computer on which you just used the USB after your use of the file or the computer had finished? Always be alert to this risk e.g. on publicly available PCs such as in hotel, reception or internet café machines, and avoid using them with anything other than a trusted, and empty/formatted USB drive. Never use a drive holding confidential information on a higher risk machine. Nor should you use such a machine to access any resource using your professional or domain account or password, because it may contain keylogger software to obtain typed security credentials.

Internet cafes

8. Whilst the use of an internet café might be appropriate to log on to a legal resource or judgement website to download and/or print public legal authorities

which would ordinarily be public and non-confidential and which would not be so practicable from a tablet or mobile phone, an internet cafe would be unlikely to be suitable for you to read or prepare confidential documents, including reading or sending confidential emails.

Charging your devices

9. Be aware that plugging a device or mobile phone into a USB connection of a third party device for the purposes of charging may expose files on your device to being read or altered. A compromised USB drive could then spread infection across computers and devices or throughout a network. If you have no choice, ensure that if options are offered by the operating system, the 'charging' option is chosen rather than any option giving file access.

10. If possible use your own clean and trusted USB charger. You should buy your charger from a reputable supplier and/or manufacturer. If there is a choice of charging using your own charger plugged into a 240/120v supply, or your own 12v car cigarette charger adapter, as opposed to a supplied low voltage USB slot, you should always use your own trusted charger rather than the USB socket in the hotel, coach, train car or bus.

Using computers belonging to others

11. Deciding whether you trust a computer will involve a number of checks, including identifying and understanding what other programmes are running on the computer, whether the computer seems to have a working and up-to-date anti-virus checker and confirming that the latest operating system updates have been installed recently. Often, unless you have full administrative access to a computer and good IT skills, you are unlikely to be able to satisfy yourself that you can trust the computer or the network to which it is connected.

12. If you anticipate that you are likely to need to access a computer when you are away, it might be better for you to take a computer that has been checked and updated by your Chambers IT provider in the UK and which has already had the very latest patches and anti-virus software installed before you leave. This is better than trying to find access to a computer at short notice which is not your own and which it might not be reasonable to trust.

13. Another advantage of taking with you a computer which has had all the updates applied is that if you were to connect that computer to the internet on a data plan for which you pay per megabyte, you would not be hit by a multi hundred megabyte automatic data download to apply the patches which would have been possible without charge on your home or chambers internet connection.

Anticipate places of particular risk

14. Busy places, including airports, provide the distraction and opportunity for confusion, separation from IT, hard disks and USB pen drives, and reduced supervision of bags. Small items, such as USB drives can be separated when coats or jackets are taken off, or in preparation for a metal detector.

15. If you use IT on a journey, for example in a train or on a plane, consider who can see your screen, its reflection, or your keyboard; consider using a privacy screen filter to mitigate the risk. Ensure you are disciplined in leaving sufficient time to close and gather any IT including USB drives well before your train stop or the plane is prepared for landing. Never leave your IT equipment switched on, logged on and unsupervised in public, even for a short time.

16. Internet cafes in all countries and in all contexts should be treated as if they are fully compromised, and you would be well advised not to use them for professional purposes, even for the purposes of logging into webmail with your chambers password.

Consider your use of credentials when accessing services from unusual places

17. Always be mindful that your use of a password through any system carries with it a risk that that password could be stored or used to access anything which is able to be accessed with the same address and password after you have finished with the computer. Everyday web browsers (such as Google Chrome, Safari and Firefox) can often be set to store email and password combinations for later use. Know where to find these settings for any web browser you use.

18. Second factor authentication (which requires you to receive and then enter a contemporaneous and further instantaneous code number or phrase on each occasion you log on) can help reduce risk.

19. Check the account or security options within any web account to see whether second factor authentication is available for that service, or ask the service provider. Be aware that second factor authentication may require you to have your UK mobile or physical possession of a dedicated second factor device or fob with you, and for it to be able to operate in the country in which you are travelling. Some dedicated second factor authentication devices use encryption technologies which are not legal for use in all countries. Some cloud providers can give support for mobile apps to provide one off authentication codes for second factor authentication.

20. For any web service or system to which you log on, if there is an option to increase security by providing an additional alternative email for notification of unusual access or security warnings, consider providing the service with a second email address or a mobile number for text notifications.

21. Consider phoning your Chambers IT support to reset passwords or to lock your account if, in an emergency, you decided that you need to use an account from a place of higher risk or on a computer which gave you any concern.

22. If there is any risk that you might have to use any professional or chambers account from a web café in a case of urgency, consider whether setting up a specific, dedicated and separate account with a different and separate password for that particular task, balancing the risk that the information in the particular task could be stored, accessed or an account re-accessed by a third party.

23. Consider what information is available after logging in with any credentials which you use when you use them away from Chambers. If you log into an account from any place or machine, consider the implications for all the data available under the account and not just for the task immediately at hand.

Border crossings, and laptops and tablets transported in hold luggage

24. There are three particular elements of risk:

> 24.1. Firstly, border authorities (including the US and Canada) have and routinely use sweeping powers at the frontier to take, copy and retain information including all the contents of hard drives, as well as to require the traveller to reveal all encryption keys. Protections accorded to your professional status as a legal professional and ordinary UK rules as to professional privilege may not apply at all border crossings. You may need to research (for any given journey) how to exercise professional privilege in relation to material held on electronic devices for the border controls at a particular frontier. For example, in relation to Canada, see https://www.canada-usblog.com/2017/11/09/are-you-asking-the-right-questions-when-you-travel-with-electronic-devices/. It may be your professional duty to refuse access and to risk being deported.
>
> 24.2. Secondly, some countries impose high import taxes on high value equipment such as computers, laptops or IT and you could be subject to those taxes if you travel without evidence that any computers are not being permanently imported (e.g. in India and Brazil).
>
> 24.3. Thirdly, corrupt officials might ask for "taxes" to be paid. Even if you are confident that the request is spurious, you might not be able to negotiate this without giving up the equipment or missing a flight. One security firm has given online the example of a Russian/Chinese change of flight.

25. The traveller needs to plan that there is a reasonable possibility that they become – at least temporarily- separated from the computer, and there is a possibility that at least a state, or a thief, takes full possession of the device. Minimising or eliminating confidential data held on any portable devices makes this risk much more

manageable; encrypting the device means that loss of the device does not automatically give access to the data it contains.

26. If you are travelling on a route where taking laptops and tablets in hand luggage is not permitted, it will be especially important to minimise the amount of confidential data which is stored on the device, given the risk of hold luggage being lost or stolen.

27. If you are confident about good connectivity from your destination, consider travelling without confidential data on your devices.

28. If possible do not travel with any copies of confidential files, unless you know that you will need to work on a particular file or set of files in the absence of reliable or trusted connectivity. Consider accessing confidential data only from encrypted cloud storage, from Chambers servers or from your own PC, as explained later in this document. You should consider configuring email software to synchronise only the most recent emails which have been sent or received.

29. If possible check with the client (if direct access), or with your instructing professional client, that it would be appropriate for you to encrypt and take a copy of the data with you before you travel. Tell the professional client which countries you intend to travel through or to with the specific data, if you know.

Further network considerations for those who cannot avoid travelling with or accessing very sensitive data

30. Always be aware that network connectivity can be compromised. Whilst it is best practice that you use secure websites (https:/) for any access, this does not entirely remove the risks associated with compromised connectivity.

31. Generally when you connect your device to a network using either a cable or the built in Wi-Fi system, the addressing is automatic. The host network offers your computer the DNS host which would then convert any familiar website name to an underlying decimal or numeric IP address. This is known as the Domain Name System (DNS). Ordinarily a user is not involved in the decision to check whether the DNS offered to and used by a device on connection is trusted or suitable. Hotel networks or public networks have sometimes been compromised by a 'poisoned' DNS configuration being given to devices.

32. For example, internet connectivity that compromises the DNS (Domain Name System) could take you to a fake website version appearing to be the ordinary website you intend to access, such as a bank or email provider. Although it might not work for your purposes, such a site could successfully capture your username or email addresses and the password you entered on the failed attempt through the fake website. That captured information could then be used by a third party for subsequent successful access to your account.

33. If you need to use a third party network (other than your own contracted mobile provider) for internet access when you are away, for example a hotel's Wi-Fi, learn how in your own device's *Settings* you can specify a particular, known and trusted DNS server rather than leave your phone or device to automatically accept the DNS server given by the hotel, conference centre or provider. Google DNS on 8.8.4.4 and 8.8.8.8 has been cited as alternative DNS provider which reduces the risk of 'poisoned DNS' attacks. Other independent DNS provision includes Cloudflare on 1.1.1.1. Both are free of charge.

34. There is increasing availability of built-in encryption of the DNS lookup process by some web browser providers. Both Chrome and Firefox now offer integrated support for encrypted DNS enquiry within their particular browser. Encrypting the DNS lookup prevents the creation of a DNS lookup log by an ISP or by the provider of a Wi-Fi connectivity within a building. Other providers, including Cloudflare, offer a partial VPN app for mobile devices to obfuscate and secure all DNS lookups by any app running on the device. The effect of this is that a hotel or office Wi-Fi provider would have a reduced immediate ability through DNS logging to summarise connection information from the device, or to identify hosts against which suspected credentials (such as your email address) might be misused.

35. Before travelling you should also make sure you are aware of any contractual restrictions associated with accessing CCDCS or CJSM from outside the UK.

Connecting back to Chambers

36. Consider asking your IT support staff about using any remote access method rather than taking confidential data with you. Use of a chambers' Virtual Private Network (VPN) or thin client system (e.g. Citrix) may remove the need to travel with confidential data, provided use of encrypted VPN technology is permitted from the country you are visiting. Take the time to understand whether your particular remote access technology makes copies of any files accessed on your local computer as you read and/or edit them, for example in a temporary file.

37. Consider checking, or asking your IT support staff to check or to keep an eye on any system or access logs whilst you are still away to ensure that any remote access use is limited to your own use at the time you made a remote connection.

38. Consider asking your IT support staff to limit the time and/or number of simultaneous connections available to any remote system using your credentials from abroad.

39. Beware of using free Wi-Fi as it may be insecure. Be aware that any Wi-Fi hotspot may or may not be provided by the organisation or carrier identified in the displayed SSID or network name.

40. If you need to access the internet from your laptop, consider whether your own device is capable of offering 'tethering' which would allow you to connect via your own trusted phone provider to the internet. Different mobile providers have different arrangements for different countries. Generally it is expensive, per Mb, but may be more secure as you can be confident that you would be using the usual UK access node (APN) supported by your own mobile carrier with which you are in contract if you have a specific need to access a handful of documents. Many mobile firms' packages and phone models have different capabilities and rules for tethering data when abroad.

41. Ask for help from your IT support, if available, to clarify whether tethering is available to you and how it can be configured, and get it demonstrated and working with your equipment and configuration before you go.

42. You can preserve the possibility of accessing confidential data while you abroad by using cloud storage or remote access software.

43. Some cloud storage providers store data using end-to-end encryption. This enables you to retain access to your data without storing it on your portable device, provided that you store the data in a folder which is not synchronised to your portable device.

44. As explained in the Bar Council's US Access: Data Protection Act Guidance, you should only use a cloud storage provider which is not directly or indirectly controlled by a US company.

45. Even if your Chambers does not offer a centralised thin client remote access system, think laterally about leaving yourself the option to connect from afar without taking confidential files with you.

46. If you don't have encrypted cloud storage or a Chambers remote access facility, consider installing a secure thin client remote access system on your UK computer, for example GoToMyPC, and then leaving the computer switched off. If, in the unintended event that you need to access confidential material, you could arrange for your UK computer to be physically switched on for the duration when you need to access it. You could then access your own UK PC from your own checked and clean UK provided laptop, securely through an encrypted 'thin client' system.

47. Provided that accessing such a secure system remotely is legal from the country you travel to, you would not have the risk of travelling with files, or having encrypted documents or software installed on your PC to which you could, in some contexts, be forced to reveal the encryption key or the access details.

48. You would want to satisfy yourself of the levels of access details required, which would likely include not only a username and password but a further password set on your chambers PC which you would have set and memorised before travelling.

49. Some thin client single machine software as a service ("SaaS") is available on a month by month basis and at an affordable level. You would need to check whether this is acceptable use within chambers before you install such direct remote access to a machine connected to the chambers network.

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 see here.