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:	June 2023
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. Your primary concern in planning Information Technology (IT) for travel should be the potential impact of the loss or compromise of any confidential information or personal data on a device lost or in a computer account accessed by a third party. 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 risks extend beyond any financial loss for replacement of a lost or stolen laptop or mobile device to reputational damage and professional conduct matters which could involve the Information Commissioner's Office (ICO) and/or the Bar Standards Board (BSB).

2. Case documents will almost always contain personal data and/or commercial, sensitive and confidential information the loss of which would impact on your professional relationship with clients as well as your reputation. Any loss or compromise may oblige you to notify the ICO and/or the BSB 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 used over a period of time can accumulate thousands of files potentially and are particularly easy to misplace given their small size. Encryption mitigates the risk that device loss causes UK GDPR breach by the dissemination and/or publication of confidential or sensitive information and consequent harm. Check that any USB device you intend to use comes from a reputable supplier and manufacturer with integral hardware-based encryption (best) or alternatively uses reputable software encryption across all the files on the device (second best).

4. Preferably choose to buy and use only a USB storage device that has been designed ground-up around encryption and security. Devices certified to the FIPS-140-2 or FIPS-140-3 standards are likely to have hardware, software, manufacturing and a supply chain adequate for professional use.

5. Be aware of the wider risk that any USB drive or peripheral poses to your phone, computer and/or Chambers' network and systems, please see the following National Cyber Security Centre's (NCSC) guidance for further information – linked here.

6. 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 where drives have a technical capacity less than their advertised or apparent size. See this article for more information – linked here.

7. Although some such drives which misreport their storage capacity may operate initially, over time subsequent files saved on the device can destroy earlier files by over-writing the same physical space. Even mainstream United Kingdom (UK) online retailers have allowed counterfeit USB device to be listed and supplied. See this article for more information – linked here.

8. Consider how you would assure yourself that it was ever safe to use any complimentary USB device given away at a legal seminar, conference or even legal IT security event given that this approach could be highly effective in identifying and targeting high-value users with highly sensitive and confidential data and/or systems believed to be vulnerable to ransomware attack. See this article for more information – linked here.

9. Mitigate the risks posed by counterfeit devices by considering carefully how and where you buy your electronic devices. Please see the following NCSC guidance for further information – linked here

10. 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. Advice about how to sanitise storage devices can be found on the NCSC website at this link.

11. For each file or group of files on the drive, consider who are the data subjects, then clarify or confirm that you can justify the risk of taking the files away from Chambers or even outside the jurisdiction.

12. If you take data with you on a USB device, external drive or mobile phone, you should only plug in the device to access the stored files from a computer you can reasonably trust. 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 may be compromised before you use it. This could compromise the privacy or the integrity of all the files on your USB device.

13. 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 personal data or 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.

Plan ahead before attempting any access from any internet cafés or from a computer you do not own and manage

14. 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.

15. Should there be a risk that you might have to use any professional or Chambers account from a web café, or someone else's computer or phone in a case of urgency, consider whether it would be best to make arrangements for the temporary creation of a task-specific, dedicated and separate account with a different username and password only giving very limited access to the material necessary for the particular task in hand and agreed by the client and/or data subject. This would be more appropriate than using your ordinary Chambers account which could represent an unacceptable risk to all the other material available within your account. Balance the

pressures of urgency you are under against the impact of account compromise through any access through a web café or a computer you do not own and manage. If you do not own and manage a computer, there is at the very least a reasonable risk that the material you access could be stored, accessed or re-read subsequently by a third party.

Charging your devices

16. You should in preference charge your phone through a lead and charger you trust and physically control (see below). 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 to the phone or device.

17. Some charging leads (e.g., Apple's lightning cables) each contain a microchip and an integral serial number which is then exposed to the phone's operating system during charging. It would be possible from the device's diagnostic data to identify which leads have previously been plugged into a specific phone. if you are cautious about how you consent to location data being collected or shared, envisage the possibility that with administrative access to diagnostic log files across a number of devices, it would be possible to deduce who had shared any given charging lead, and to cross reference geolocating data showing where other phones were when they were being charged by the same lead where users of those other phones being charged had previously consented to a wider sharing of their own location data than you may have done. Consider only using your own charger and lead when you travel, particularly if your travel, work or profile has attendant security risks.

18. See this link, for information on the 'MFI Made for iPhone' hardware assurance system and associated licensing is part of that supplier's efforts to ensure supply-chain integrity and reduce the risk cause by bad actors (please see further information at this link).

19. For reasons of electrical safety, as well as IT hygiene, it's best to use your own clean and trusted USB charger and lead when you travel.
You should buy your charger from a reputable supplier and/or manufacturer. See this article for more information – linked here.

20. 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. If you intend to use a public, hotel or train/plane USB port or for charging, buy yourself a USB protector. Please see this article for more information – linked here.

Using computers belonging to others. Apply app updates before you set off.

21. 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. If you intend to use a web browser, establish the version of the browser before you use it. Often this is found under the *Help*, *About* menu – which also often confirms that updates to the browser have been successfully applied.

22. 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.

23. Check within the application store icon on any mobile device (e.g., the blue 'App Store' icon on an iPhone) as to whether there is any backlog of apps on your phone or device which still need to be download and/or applied before you set off. This gives you the opportunity to be confident your apps are up to date and working before you set off. This can also avoid your wasting gigabytes of any finite data allowance if you were to delay doing this until you are away from Wi-Fi at home or in Chambers.

24. Familiarise yourself with any data use minimisation options for your phone. With the frequency of large multi gigabyte overnight updates, any inclusive roaming allowance may be quickly exhausted if you installed every possible update for every possible app when abroad and only using mobile data. Do make checks for app updates routinely when you are connected to a Wi-Fi you trust.

Anticipate places of particular elevated risk where you might be separated from your devices or where you your screen, device or passcode can be seen.

25. Busy places, including airports, provide the distraction and opportunity for confusion, separation from IT, hard disks and USB devices, 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.

26. 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.

Consider your use of credentials when accessing services from unusual places.

27. 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) or installed add-ins 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 and check for installed add-ins or extensions if you use a web browser on a machine which is not your own.

28. Be particularly careful if your Touch ID (fingerprint) or Face ID (facial recognition) fails to work in a public place, and you are then prompted to enter in a full device passcode in public or within sight of a camera. For example, at a busy bar or in a queue. This has been used to give subsequent access to the whole device and all the apps, including banking apps and any password manager.

29. There have been recent examples of targeted organised attacks characterised by a separation in time between someone observing the user entering in a phone passcode in a busy place, and subsequent physical theft of the device by a different actor. The rapid use of the observed passcode by another actor very shortly after the theft is used to reset the account to prevent the user having any further access to the cloud account in the moments whilst the victim is still in the busy place being observed and still unaware that they are no longer in possession of their device. The attacker gains complete access to the device and apps within the device. The user was then quickly locked out of their own cloud-based account to report the device as lost or stolen or to contact financial institutions about the theft of their identity. In some cases, high value international money transfers emptied the victim's bank account by virtue that the financial apps also trusting the overarching ID in conjunction with text messages to the stolen phone. Be cautious about where and when you use any code to override

biometric identifiers and gain access to the whole device. Please see further information in this article – linked here.

30. Multi 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) reduces risk. Using different passwords for different services reduces risk and is recommended.

31. Check the account or security options within any web account to see whether multi factor authentication is available for that service, or ask the service provider. Be aware that multi factor authentication may require you to have your UK mobile or physical possession of a dedicated multi factor device or fob with you, and for it to be able to operate in the country in which you are travelling. Consider installing an Authenticator app on your mobile device, such that one-time passcodes for relevant services such as your email account or a particular service can be generated dynamically on a known device you trust, rather than sent through as an unencrypted SMS message. Some dedicated multi 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 multi factor authentication.

32. 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.

33. 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. 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

34. There are three particular elements of risk:

35. Firstly, border authorities (including the United States (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.

36. 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. It may be your professional duty to refuse access and to risk being deported. For example, in relation to Canada, please see this article – linked here. The Canada Border Services Agency ("CBSA") has published a written statement on its website that when the CBSA conducts an examination of electronic devices (e.g., laptops, smart phones, USB keys, etc.) at the Canadian border, CBSA officers must not search electronic documents marked as "solicitor-client". See "Examining Digital Devices at the Canadian Border" for information – linked here. 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).

37. 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. 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.

38. 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.

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

40. 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.

41. Where 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.

42. 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.

43. When you connect your device to a network using either a cable or the built in Wi-Fi system, the addressing is generally 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.

44. For example, internet connectivity that compromises the DNS 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, albeit with warnings popping on the device. That captured information could then be used by a third party for subsequent successful access to your account.

45. 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. On an iPhone this is as simple as clicking on the information I icon once connected to a Wi-Fi network, which then allows you to change the automatic DNS provider to a manual one that you trust, e.g., 1.1.1.1 for Cloudflare.

46. 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 profile device use, or to identify hosts against which easily-guessed credentials (such as your email address) might be misused to attempt access.

47. Before travelling you should also make sure you are aware of any contractual restrictions associated with accessing HMCTS' digital systems for courts and tribunals – including the Crown Court Digital Case System (CCDCS), Common Platform or the Criminal Justice Secure Email (CJSM) from outside the UK.

Connecting back to Chambers

48. 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.

49. 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.

50. 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.

51. Beware of using free Wi-Fi from untrusted providers. Avoid using unencrypted Wi-Fi. Take note of any security warnings your devices give you when attaching or using any unfamiliar Wi-Fi service. Be aware that any Wi-Fi hotspot may or may not be provided by the organisation or carrier identified in the displayed service set identifier (SSID) or network name.

52. 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. Know and monitor your inclusive data allowance on any mobile plan. Generally, use beyond the inclusive allowance 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. Familiarise yourself with where these settings are found on your device.

53. 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.

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

55. 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.

56. 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.

57. 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.

58. 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.

59. 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.

60. 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.

61. 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 for accessing Chambers' systems before you install such direct remote access to a machine connected to the Chambers network.

Consider your power supplies

62. In view of the uncertain energy security situation in late 2022, take some thought as to which battery systems, or 5v charging systems are available to you. Inexpensive battery backs can charge your mobile multiple times. Information available and synchronised to an iPad or tablet would continue to be available for a longer period in the event of a power failure. If you arrange your mobile devices appropriately, they will also function to mitigate power loss risks. Consider whether there is a general advantage to getting a mobile device such as a laptop ready and fully working and freshly synchronised with relevant Chambers files, so that you could use this device for some hours in the absence of mains power to you, to Chambers, or to the networks or systems which support these services.

63. Check the Bar Council's advice on Back up Work on your PC and consider arranging for your laptop to have an email client (such as Outlook from Office 365) configured in such a way as to have access to the last year's emails sent and received but stored within a locally available data file. This might allow you to get quite a lot of work done in the temporary absence of connectivity or power, or servers.