THE GENERAL COUNCIL OF THE BAR
JUSTICE FOR ALL

Windows 10 Security Advice for Apple Macs

Purpose:	To guide all barristers on security issues relating to the Windows 10 upgrade on Apple Macs
Scope of application:	All practising barristers and chambers
Issued by:	The Information Technology Panel
First issued:	April 2017
Last reviewed:	October 2020
Status and effect:	**Please see the notice at end of this document. This is not “guidance” for the purposes of the BSB Handbook**

Using Windows on your Mac

1. Most Mac Users would not really see any reason to use Windows 10 on the Mac but those who wish to do so have the following options.

2. Any Mac user requiring access to the Windows environment could use a ‘thin-client’ technology[1] which would give access to a remote Windows system without Windows being installed on the Mac itself. Some sets of Chambers, as well as instructing solicitors working on specific cases, do offer thin client access (e.g ‘Citrix’) for the use of Windows-centered document retrieval systems and for use with specific case management systems and/or bundles. The advantage of using a thin client, if it is available to you, is the simplicity of installation, and that the integrity of the Windows environment and the security is then the responsibility of your provider.

3. Another option for running Windows on the Mac is by using virtualisation programs (such as Parallels Desktop, or VMWare Fusion) which create a ‘virtual machine’ that runs within MacOS itself. The virtual machine is simply an app that

[1] Thin client technology runs from resources stored on a central server instead of a localised hard drive. Thin client work by connecting remotely to a server-based computing environment where most applications, sensitive data, and memory, are stored

runs on the Mac just like other Mac apps. However, the virtual machine mimics the workings of a PC, allowing you to install Windows on the virtual machine. But as you will be running your Windows on the virtual machine with your Mac simultaneously, you will need sufficient memory and processor power in order to provide decent performance. The majority of the time using the virtual machine will be slower than an actual PC with its own built in processor and memory. This is where Boot-Camp Assistant, provided by Apple, may be the best option for Mac users who want to install Windows.

Boot-Camp Assistant

4. Mac users who want to install Windows 10 on their own Mac might choose to use "Boot Camp" Assistant (a multi-boot-utility) to assist in installing Microsoft Windows 10 on supported Mac models. The Boot Camp Assistant partitions your Mac's hard drive into two parts, one partition for the MacOS and installs Windows on the second partition. This enables you to simply choose when you switch on your Mac which operating system (MacOS or Windows) you want to use. You cannot use them simultaneously as you need to work within one of the partitions at any given time. Newer Mac computers use a streamlined method to install Windows on your Mac. To find out whether your Mac uses this method, see the Apple Support article Install Windows 10 on your Mac with Boot Camp Assistant. If your Mac is an older model, follow the instructions in Install Windows on your older Mac using Boot Camp instead.

5. You need a Microsoft Windows disk image (ISO) or installation media containing a 64-bit version of Microsoft Windows 10. Boot Camp Assistant supports 64-bit versions of Windows 10 when used on a supported Mac. An ISO file is a single file which is a complete representation of an entire CD/DVD. If you purchased the USB flash drive version you can download an ISO from Microsoft and use the Windows installation key that came with your flash drive. If you're installing Windows for the first time, make sure the Windows installer you're using is for a full installation (not an upgrade installer). Obviously make sure you back up all your files and data before installing the software.

6. Before installing Boot Camp it is important you:

   a. **back-up your files and data**. For information about backing up files, see Back up your files with Time Machine and Ways to back up or protect your files.

b. **check you have the latest software updated on your Mac.** The latest Mac operating system at the time of writing is macOS 10.15, also known as macOS Catalina[2]

c. **check you have sufficient memory** in order to install Windows 10 alongside your existing Mac Operating System (with a minimum size of 64GB partition, 128 GB is recommended for best experience).

7. For full instructions on installing Windows on your Mac using Boot Camp see Apple's Boot Camp Assistance User Guide[3].

8. The IT Panel's documents: "Windows 10 Upgrade Advice" and "Cloud Computing" each contain useful points to consider when using Windows 10. In particular, you should check the following:

a. Whether any of the Privacy Settings have been altered on your Mac once the installation of Windows 10 has been completed, to make sure that you do not, for example, provide samples of your writing style or vocabulary that could inadvertently lead to a breach of client confidentiality. You should check your privacy setting not only on the Windows 10 control panel, but in the "Security & Privacy" section of your "System Preferences" as well. Similarly, you should consider whether to use Cortana as the terms of use for the voice controlled "digital assistant". Cortana requires a considerable degree of data export and analysis of your contacts, messages and pictures. As you install Windows 10, choose the "Customize settings" option and step through the "Privacy" options. If you did not choose to customise the Privacy options as the update was installed, make sure you review the Privacy options through the "Settings" option after the upgrade.

b. That security provisions are in place for any cloud-based computing you choose to use. The issue of document file storage (as opposed to the storage of settings in the cloud) is dealt with in the IT Panel's document on use of cloud services (available here).

Safety Features on Macs

9. For information on Apple Platform Security visit the Apple Website[4]. Apple system security encompasses the boot-up, software updates and ongoing operations of the OS. The most recent versions of iOS, iPadOS or macOS are the most secure, so the best way to keep your Mac secure is to run the latest software and keep it updated. "Runtime protections" limit access to system locations and restrict access to system processes which supports a security policy guarding against compromise, regardless of any administrative. Mac computers with an

[2] As checked on 12 October 2020 when this Guidance was updated

[3] https://support.apple.com/en-gb/guide/bootcamp-assistant/bcmp173b3bf2/mac

[4] https://support.apple.com/en-gb/guide/security/welcome/web

Apple T2 chip (latest versions) ensure that only legitimate MacOS operating system software loads on the Mac, but in all cases you should only use the approved apps from the App Store.

10. As well as the MacOS alerts giving warnings on potential infected files containing malware before you open them, the following safety features complement safety:

11. For Apps:

a. Apple has its 'Gatekeeper' that builds on OS X's existing malware checks to help protect the Mac from malware and inadvertently installing malicious software. Gatekeeper has three security options, the default option allows the user to download apps from the Mac App Store as well as those developed by Apple identified developers (Developer ID having been issued from Apple). If an app is unsigned without a Developer ID the user is informed and allowed to choose to manually override Gatekeeper if they so wish. It is advisable not to override the Gatekeeper.

b. Apple's Sandbox in macOS blocks malicious code. App sandboxing isolates apps from the critical system components of your Mac and your other apps. Even if an app were compromised by malicious software, sandboxing would limit that compromised app's ability to interfere with the working of the Operating System or other apps. You would still be vulnerable to information loss if you authorised a compromised app to access any set of data, such as your contact list. Sandboxing will only limit the effect of your downloading a compromised app. You should always satisfy yourself that any app installed is necessary, likely to have the intended functionality and comes from a reputable source. Further, you should restrict the access any app has to data which is otherwise shared across the system, such as contacts, photos, documents, the camera and the microphone. Many apps request location data, either when they are in use, or all the time. You should be cautious in deciding which apps require access to your location data, and whether you grant access only when you are actively using the app or all the time.

12. For encryption: Apple has FileVault 2, which is used to keep data safe and secure. FileVault 2 encrypts the entire drive on your Mac, protecting your data with XTS-AES 128 encryption. On Mac systems with an Apple T2 chip, Filevault 2 keys are created and protected by the Secure Enclave. Go to 'Security & Privacy' Settings in 'System Preferences' to make sure you have turned FileVault 2 on.

13. Regarding Privacy Settings, System Preferences contains privacy controls for location sharing and diagnostic information sharing. Further Safari preferences include a privacy panel that allows you to limit or block cookies and limit website

access to location service. These all should be regularly checked. Safari also has anti-phishing technology inbuilt.

14. While no system can be immune from every threat, macOS does provide you with easily configurable options and decisions to help you improve your approach to overall information security. You will find most of these additional security features in the "Security & Privacy" panel of the System Preferences. A few recommendations would be:

a. Confirm that your firewall is switched on to prevent other machines from accessing services running on your Mac.

b. Do not use public WiFi without a VPN and be vigilant to phishing attacks by implementing cybersecurity rules of use

c. Restrict physical access to your Mac by setting the screen to lock with a password, or ensuring that TouchID is required after a period of inactivity.

d. If you need to set up file sharing, set it up securely with two-factor authentication where possible

e. Use Password Assistant to create stronger passwords for local utilities like Users & Groups. Use a two-factor authentication process where possible.

f. Make sure you are only running sharing services that you really need.

g, If you have a capable MacBook, consider using Touch ID as an additional security safeguard.

h. Take steps to understand the implications of offers by any web browser or system to save username and password data for websites. Typically these can be stored in the Cloud and then replicated across your devices. Subsequently anyone with access to any of your other devices could in theory then access restricted websites if you had earlier chosen to save such browser passwords to the Cloud.

i. It is good practice to consider using two-factor authentication for any services which could use more than a username and password for access.

<u>Important Notice</u>

This document has been prepared by the Bar Council to assist barristers on matters of IT. **It is not "guidance" for the purposes of the BSB Handbook 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.