CornerStone
Computer Centre (Est.1997)
The Arcade, Bognor Regis
West Sussex, PO21 1LH

Microsoft Registered Partner
Director Michael Corner

01243-820082
07919-376677 (text ONLY)
support@CornerStone.me.uk
www.CornerStone.me.uk

Important Information For macOS Users

macOS is Apple's proprietary alternative to Windows or Linux. Although based on the same technology as Linux (apps can be cross-compatible with Linux), macOS has little better than a micro-kernel, supporting very little hardware, whereas Linux uses a monolithic-kernel, supporting vastly more! Generally, operating systems (e.g. macOS, Windows, Linux, etc) contain 3 main components: kernel, distribution & desktop (there's separately also device drivers (some are built-in to kernel), software & data files)... Unlike Linux, in macOS & Windows, these are bound into 1 item & are not individually upgradable or customizable (generally, just colours, fonts, icons & background picture).

We always use the same username & password (for login & keyring) for macOS: username=*owner*, password=*1234*.

Apple don't provide or supply installation media to install macOS, so only the newer (2012+) computers (with Internet Recovery) are worth installing macOS onto. For older computers, since they won't be compatible with a supported version of macOS anyway, Linux is recommended instead (MUCH faster, safer & more compatible than macOS with over 300 versions to choose from). After turning on computer, wait for the 'tones' then hold *Option* + *Command* + *R* to start *Internet Recovery*. When loaded, you'll need to goto *Disc Utility* to prepare the HDD/SSD (either create partition(s) or volume(s) or erase) & then can select *Install macOS*. It'll take a LONG time, far longer than the minutes 'estimated' on screen, so just be patient!

Although built-in to macOS, it's HIGHLY recommend to NOT use *Safari* or *Mail* - they're both EXTREMELY unsafe & are an easy way to get infected. It is VERY rare for us to see an uninfected macOS computer, however, having good anti-virus, a safe web browser, a secure email program & keeping ALL installed software up-to-date, significantly reduces the risk of infections.

After installing all available updates, we install the following programs (if compatible with the version of macOS installed):

CornerStone Premium Software Suite:

Avira: Block & remove viruses, malware, spyware, etc & firewall to stop attacks... CRITICAL to keep up-to-date	**Bitdefender**: Passive scanner to remove viruses, malware, spyware, etc that may have slipped through active security	**Malwarebytes**: Passive scanner to remove malware, spyware, etc that may have slipped through active security
Opera: fast & secure web browser with built-in ad-blocker, VPN, speed dial, chat messengers & lots of available plug-ins	**Skype**: internet chat & reduced rate computer to telephone calls	**AnyDesk**: remote control of another computer - we offer support at £5 per 10 minutes
LibreOffice: Microsoft compatible word processor, spreadsheet, presentation, desktop publisher & database	**Mozilla Thunderbird**: secure email client with spell checker, anti-SPAM, anti-phishing, automatic updates & customizable interface.	**Commander One**: twin window file manager

Not included, but popular optional programs:

Spotify: stream music from millions of available tracks	**Dropbox**: store, sync & share files in the cloud	**Microsoft Online Office**: Microsoft's web based versions of Word, Excel, PowerPoint, Outlook, etc
Send Anywhere: allows sending/receiving files between Linux, Windows, Android, macOS & iOS	**qBittorrent**: Torrent client - goto unblockit.lat or use a VPN to access blocked websites	**Steam**: online gaming platform with 1000's of available titles
Krita: image editing, similar to Adobe Photoshop or Corel Painter	**Shotcut**: non-linear video editor - includes capture & visual effects	**VLC**: media player with many built-in codecs for CD/DVD & audio/video files

1. If using a router for internet connection & it was already setup & previously in use, do NOT install ANY software from internet provider (it wouldn't be required & is unlikely to be compatible with macOS anyway!) – nothing more is required to reconnect to internet. macOS connects EXACTLY the same way Windows or Linux would... If using a network cable (8 pin, RJ45 plugs) from router, just plug it into a LAN port on the computer & you're connected (same as Windows & Linux). If using built-in wireless connection & it didn't auto-connect (if it did, that would mean you have an unsecured router with no wireless password setup, so anyone nearby could use your internet for free(!) - potentially this could cost you a lot of money if you have a usage limit & they take you over &, at the very least, they would slow down your internet speeds!), click network connection icon by clock & it'll display in-range routers/networks (if yours isn't displayed, check router is plugged in, switched on & LEDs are lit & if still not listed, you're either out-of-range, so move computer closer, or there's a fault with the router or service, so contact your provider), select yours from list, enter the router's current wireless password (either password entered when router was setup or whatever was assigned by internet provider - often either printed on router or supplied on a card (if you're unable to read this, either use a magnifying glass or take a picture with a smart phone or digital camera & then you can 'zoom in' to make the writing bigger!)) when prompted & you're connected (same as Windows & Linux). If you change router's WiFi password, you'll need to remove it from stored networks so macOS (& Windows & Linux) will re-ask (click network connection icon, Open Network Preferences, Advanced, select connection, click "-" to remove & then reconnect as per above). If you're starting afresh with a new router, it may need to be setup before use (check ISP's supplied instructions). If using 3G/4G/5G USB modem, plug it in, click network connection icon & select mobile network (may be named, e.g. Vodafone), then follow prompts to select internet provider & service type (contract/PayAsYouGo) & it'll automatically connect (NOTE: some modems/providers require entering details for APN, username and/or password (e.g. Vodafone password is *web*), so you might need to check with provider). If you have a MiFi or use tethering from phone/tablet, connect as per wireless above. If macOS has been reinstalled or you previously had Windows/ Linux installed or you have a different computer to before, then it won't yet know your router & password until you tell it... It's a one-off procedure, that you did in exactly the same way previously, when you first connected your computer to that router & after, macOS 'remembers' it for next time. **Until connection is (re)established, you CANNOT browse internet, check email, search, download, update ANYTHING from the internet** (same as Windows & Linux)! If you've forgotten your WiFi password, you can't find out what's stored on the router, but you can change it (a router reset 'might' return it to whatever the default was, but could also just wipe it & you'd need to re-setup the router). Router access details & default password(s) are either supplied with the router or printed on a sticker on the router. Plug a network cable (should be supplied with router, else we sell 2m @ £2.50) into router & computer (some newer portable computers don't have a network socket, so you can't do this with them!), load a web browser (e.g. Opera), enter router's IP address (e.g. 192.168.0.1), enter router's login details, browse to WiFi/WLAN/etc settings, delete the current WiFi password & just enter/make up a new one (then write it down & keep that somewhere safe!), save settings & then connect as per above. Any other wireless devices (e.g. mobile phone, other computer, TV, etc) will need to reconnect with this new password.

2. For wireless security on your router, make sure you're using at least WPA2 encryption (check router's manual for how to access settings). WEP (slow) & WPS are both easily 'crackable' & WPA1 isn't encrypted at all! Additionally, always change the default router name & password as there's software available to display default passwords based on router name. If someone (nearby) can access your router & they use your internet, YOU could be faced with a large usage bill if they take you over your limit. It's illegal (fines & prison) & you should report such activity to the police!

3. To run a program in macOS, do EXACTLY the same as Windows or Linux... shortcuts on desktop are double-left click to run, shortcuts on menu or dock (if present) are all single left click (unless mouse/touchpad is set to left-handed mode, in which case left & right are reversed). To exit a program, again, do EXACTLY the same as Windows or Linux... left click [x] in top left or right (depending on theme/program) edge of program window, or program may have a menu with Quit/Close/Exit/etc.

4. Similar to Linux, Apple's macOS uses a 'keyring' to store passwords (for example, in web browsers for remembered website logins). The keyring too has a password & our default is the same as the user password: *1234*. Files (e.g. documents, pictures, etc), like Windows & Linux, can have "read-only" permissions, preventing overwriting or changing... to change: right click file, select Properties, Permissions, change access for required group(s) to "Read and write".

5. Similar to Microsoft, Linux & Android app stores, macOS uses a software 'repository' called *App Store* – this lists all available programs (older versions of macOS are unlikely to be compatible with newer software) & you can just browse or search to install any program (click *Get*)... be mindful, a program that is free on other systems, may NOT be free on macOS! Software can also be installed from CD/DVD or downloaded from the internet, but make sure you're on a trusted website (e.g. for Epson printers, goto www.epson.co.uk).

6. If you had requested a data backup, then your data files (i.e. documents, pictures, music, videos, downloads & fonts) will either be reintegrated, for single user backups, or stored in a folder called "My Backup", in the downloads folder. This folder will also contain any other files that can't just be 'copied back'.

7. macOS is able to install & run Windows based programs (do NOT try to install hardware device drivers this way)... To install Windows software, use *Wine* & *PlayOnLinux* (if not already present, install from App Store & if it's in the supported program list, just select it to automatically download & install the program for you. For anything else, try installing the downloaded ".exe" program, as you would in Windows (it'll use Wine), but be mindful not everything will be compatible.

8. Since most infections are web based, a safe web browser, correctly setup, is absolutely CRITICAL to limit attacks. We recommend, install & setup Opera, which has a built-in popup & ad-blocker (making browsing faster & safer), a VPN (Virtual Private Network, to access websites blocked by region), speed dial (like bookmarks, but bigger & often with website logo for quick & easy access), secure DNS lookup (preventing 'man-in-the-middle' attacks), popular chat messengers (e.g. Facebook, Instagram, Twitter, etc) & lots of available plug-ins (to add additional functionality). Try to avoid Safari & Chrome as they're EXTREMELY unsafe & incompatible! **Whichever browser you use, it is highly recommended to use it's online synchronization feature** (included in most modern browsers) **to save your favourites/bookmarks/settings/passwords/etc online**... This allows access between different computers & ensures you wont lose them when hard disc drive (or solid state drive) fails! Anything entered into the address bar, which isn't a web address, is deemed to be a search. We set the default search engine to be DuckDuckGo, which uses Yahoo (by far, the best), but with no tracking & supports filters for where (e.g. UK) & when (e.g. last day/week/etc). Since Google call themselves a "Content Provider" NOT a search engine, they will only show results where they received advertising revenue! Microsoft's Bing also uses Yahoo, but is pre-filtered to show less. Yahoo Search has been bought by Oath, who keep informing you Yahoo is now part of their services whenever you search, so quickly becomes annoying!

9. To access email (after (re)connecting to internet (see above)), you'll need to know your email address & password to login. If you've forgotten your email address, ask someone who's previously sent you an email to tell you what address they used. If you've forgotten your password (case sensitive, so "abc" is NOT the same as "ABC") then, via a web browser, goto the email service website (e.g. outlook.com, talktalk.net, etc) & click "Forgot password" (or words to the effect) on the login page to reset your password (they may text a code for you to enter or send a link to another email address or ask security questions, depending on what information you gave when originally setting up the email address & after confirming, you can create a new password). ALL email has ALWAYS had a password to login... previously, you may have instructed your web browser or email program to remember these details & enter them for you after the first time you logged in - you can do the same again, once you login this time. If you use a 'web based' service (e.g. Yahoo, Outlook (the new name for Hotmail) or Gmail (NEVER send confidential emails via Gmail as Google sell them & say people will be reading them!) then it's not stored on your computer so you just go to their website & sign-in to access your email & contacts as before. If you used 'client based' email (e.g. Thunderbird, Microsoft Office Outlook, Mail, etc), you'll need to re-enter your email account details (e.g. email address, password, inbound/outbound mail servers, etc) & then you may be able to import your contacts & old emails from the backup folder. Most internet providers include help on their website on how to do this. Ideally, always use webmail (e.g. *outlook.com*) so when you change ISP, you don't lose email address (e.g. yourname@talktalk.net). For SPAM email, NEVER unsubscribe else you've confirmed address is 'live' & you'll get far more & malicious emails! Webmail never needs to be backed up, you can access it from anywhere on world & you can't get infected from malicious attachments unless you manually download & open them!

10. Unlike Linux, macOS has limited hardware support built-in, so for the vast majority of devices (e.g. WiFi, Bluetooth, printer, scanner, webcam, etc), like Windows, you will need device drivers installed (check manufacturer's website). Also, not everything is compatible!

11. If hardware (e.g. printer, WiFi, etc) isn't working, check the obvious first: is it plugged in? Is it switched on? Are the lights on? Is it installed/setup? Is it enabled? For notebook/laptop computers, it's common there's a key to enable/disable WiFi, so if not listing any networks, check it's turned on!

12. Universal Serial Bus (USB) is an industry standard specification for cables & connectors for communication & power. There are MANY different plugs & sockets (e.g. A, B, C, mini, micro, lightning, etc) & different devices (e.g. computers, tablets, cameras, telephones, etc) & manufacturers (e.g. Apple) use different (sometimes proprietary) sockets & each has a different name (so you know what to buy as "USB to USB" says nothing about the plugs or sockets!). Printers use USB A to B plug cables. Computers generally have USB A sockets, which, without a separate convertor, don't carry video & two computers can't be linked together.

13. Unlike Windows' monthly updates, or Linux's often weekly or even daily updates, macOS updates can be very infrequent, but you'll be alerted (via an icon by clock or on dock) when any are detected. These should be downloaded & installed as soon as possible. Updates can fix security issues, add new features or improve existing ones, but, unlike Windows updates, like Linux, macOS updates also include all installed programs!

14. Google themselves say they're NOT a search engine(!) & haven't been one for many years - they call themselves a 'content provider', displaying mostly sponsored links. You'll often see the "did you mean..." message. However, virus writers & scammers pay Google for links to malicious websites, so check the link looks genuine before clicking it. The results you get from Google searches are filtered based on your previous searches & whatever other information they have stolen from you(!) to show the results they can make the most advertising revenue from! Yahoo, Bing (both filter, but not to the extent Google does) & DuckDuckGo find substantially more applicable hits & are far safer, but since DuckDuckGo record & track nothing (so every search is a 'first' search), have selectable country, filters to omit adult content & search by time, they are the recommended choice. Most of the information on the internet is either out-of-date or just plain wrong(!), so finding current & accurate information is made much easier with DuckDuckGo.

15. Individual data items (e.g. documents, pictures, music, videos, etc) are called, "files" & are stored in containers called, "folders". It makes sense to name them based on their content & to store them in appropriate folders (e.g. a Christmas shopping list called, "today" stored in the "Pictures" folder wouldn't be quick/easy to later locate). Folders can themselves contain folders, so files can be compartmentalized for better grouping by category (e.g. in "Pictures" folder, a folder called "Holidays" which in turn contains folders for years or places, which contain those pictures). It is bad practise to store files or folders on the Desktop as this will reduce computer performance (Desktop folder is refreshed frequently) & it's all too easy to accidentally delete something by mistake! In addition, if you fill the Desktop you won't even be able to see new items, let alone open them!

16. The world's greatest internet threat is the rise of ransomware infections - these encrypt all your data files & then demand £100's (sometimes £1000's!) payment within a short time to decrypt them else they are permanently lost! They are mostly distributed by email & malicious websites (accessed by Google 'search' or malvertising (fake adverts)). **ALWAYS backup important files & make sure all installed software is kept up-to-date**.

17. Before clicking on a link to goto a website or downloading ANY software, check the link on the browser status bar matches a 'likely' address... look for "/" at the end of the web address & before a web page as 'phishing' sites will often use mis-spellings of well known web addresses or have extra text on the end of the address before the "/" (e.g. www.bbc.co.uk/radio2/guide is ok, but www.bbc.co.uk.radio2/guide is not!). When installing, select setup/custom/options/advanced/etc to untick/exclude unwanted settings or other included software. These are common methods for how adware/malware gets installed.

18. When signing into a website (e.g. email, banking, shopping, etc), if website says email address or password are incorrect, this means, however sure you were that you'd typed them correctly, you've typed one of them wrong! Although email isn't case sensitive (e.g. FredAndGinger@hotmail.co.uk is ok), passwords are, so carefully check what you're typing & try again. If you've forgotten your password, generally it can be reset if originally, for that website, you supplied a telephone number and/or another email address that you still have access to (they'll text or email you a code or link to confirm you're the account holder, so you can change the password). It's a good idea to write down your passwords in a book, in case you forget one. It's often recommended to have different secure/long passwords for every website, but in practice this is pointless, so the same, easy-to-remember password for any non-critical websites (not email or financial) & then secure/long just for those that need it.

19. Most of the computers we see with virus, spyware or malware infections got infected via Facebook, Google or email! Due to their popularity, they are specifically targeted by virus writers & scammers. To reduce the chances of being a victim, if something doesn't look right, or it seems suspicious, then it most likely isn't safe, so don't click on it!

20. We get a lot of customers telling us they've had callers, often saying they're from Microsoft or BT, claiming to have detected infections or problems on their computer & asking to allow access - which they use to upload programs or infections to support their claims – it's a scam that often costs £100's! Just say you don't have a computer! If you've already been a victim of this scam, contact the police & report it to your bank – you've been robbed!

21. Secure websites should show a padlock symbol before website address in address bar of web browser, else you might be on a 'phishing' website, masquerading as legitimate & trying to steal your login credentials! It's good practice to use strong passwords (i.e. mix of upper & lower case letters with numbers &/or symbols), but most people would find them hard to remember, so either use a password manger or it's built-in to most web browsers to store them or, write them in a book & store that safely not next to computer (if someone break's into your house, they're more likely to take your computer than your passwords book!). For non-secure websites (i.e. requiring no personal or bank/card details), you could just use the same email & password for all as there's no financial implications. For an easy way to remember long passwords, use a phrase or a line from a song or poem you know well, so aren't likely to forget. To check if your email address has been involved in a data breach, goto: haveibeenpwned.com

22. Computers can playback CD, DVD, Blu-ray, etc & audio/video files (proving you have appropriate hardware & software) to the connected speakers/monitor, which can be internal (as in a notebook) or external (as on a PC) & even to multiple screens (e.g. notebook to TV)... Increasingly, devices are supporting WiDi (Wireless Display) output to compatible screens (mostly smart TVs), often going via an internet connection using your router. This is known as 'casting', 'screen mirroring' or 'streaming'. Quality of playback depends not just speed of computer, but also WiFi signal strength & internet speed. Non-smart TVs can use a 'cast' device such as Google Chromecast or Amazon Fire Stick (MUCH better & cheaper!) & these also allow installing 'apps' like BBC iPlayer. Casting output can also be achieved by software (e.g. built-in to Opera web browser). Setup requires 'pairing' (like with Bluetooth) but once done, compatible computers, phones, tablets, etc can display any output on another (often bigger) screen.

23. Deleting data files or uninstalling programs which are not always running in the background, will free up disc space, but will have zero impact on computer performance, unless disc was almost full with only megabytes of available space. Manually deleting (rather than uninstalling) programs is liable to make macOS (& Windows & Linux) unstable & can even prevent booting! Don't set any data backup to save to the same drive (as completely pointless in the event of drive failure!) & limit the number system snapshots (via Time Machine) to no more than 3 (can restore entire system in the event of corruption).

24. Dust gets into computers & clogs up fans & air vents causing components to overheat & if temperatures get too high, they'll burn out! This can often be a costly repair, sometimes more than computer is worth! Check regularly for dust build up & clean when necessary. Thermal paste (between chip & heatsink) should be replaced if dried out. If portable computers have air vents on base or contain mechanical (rather than solid state) hard disc drive, then they're a 'notebook' NOT 'laptop' & MUST be used on flat & steady surface to limit overheating & drive damage (movement, while powered, causes heads to hit disc surface, damaging disc!). Since batteries are for portable use, after charging (ideally, not more than 80% & don't let it go lower than 5%, which can double the battery life expectancy!), remove when mains powered (switch off first!) else computer will actually be reducing battery capacity! Top up battery every few months to keep it 'alive'. Modern Apple portable computers are laptops & the battery is screwed in on the inside, so can't easily be removed, meaning it'll constantly be killing it, reducing it's capacity!

25. Any important files (e.g. documents, pictures, music, videos, etc) should be 'backed up' each time they change – if you work on your computer weekly, then you backup weekly, if you work daily, then you backup daily! ALL hard disc drives fail – no exceptions – & infections/attacks can corrupt files! Make copies on external hard disc, USB flash drives or online storage, but ideally, not CD/DVD/Blu-Ray discs (short life span & unreliable).

26. CornerStone Computer Centre sell ink cartridges (inkjet or laser), at the lowest prices (by far!) in the area. We keep large stocks of Epson, Brother, Canon & HP individual inks. Printers with only two cartridges, with all the colours in one cartridge, should be avoided... when you run out of one colour, you've lost the others as they're in the same cartridge! Inks for these printers are generally 10x more expensive than individual inks (commonly £2-£4), so NEVER buy a two cartridge printer & if you already have one, when the inks run out, just buy a new printer as it'll save you a LOT of money on the running costs!

Thank you for using CornerStone Computer Centre.
This document gets updated frequently - the latest version is available via our website.