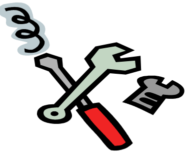
CornerStone
Computer Centre (Est.1997)
Bognor Regis / Bersted, West Sussex

Microsoft Registered Partner
Director Michael Corner

07919-376677
support@CornerStone.me.uk
www.CornerStone.me.uk

Important Information For macOS Users

If you brought a PC (rather than notebook/laptop) in for servicing then, when plugging leads back in, almost all can only fit in one socket & only one way around! Speakers (green) & microphone (pink) could be connected incorrectly (it wouldn't damage them, but they wouldn't work unless 'soft selectable' & you're prompted for function), but plugs & sockets are often colour coded to help. Make sure all plugs are inserted firmly (some 'click' & some have thumb screws), but don't force any. It's common there's an on/off switch at the back of PCs, so make sure it's switched on! If you've NOT just had macOS installed, you can skip ahead to paragraph #9, though you may find it informative to read the rest anyway!



Apple's proprietary alternative to Windows or Linux is *macOS*. 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).

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*. This will download the latest version of macOS your computer is compatible with. Alternatively, *Command + R* will download the most recent version of macOS you previously had on your computer or *Shift + Option + Command + R* download the version of macOS that originally came with your computer, or the one closest to that version if it isn't available as a download. Note: if you're selling or giving away a Mac that is using OS X El Capitan or earlier you should use *Command + R* - this will make sure that the installation isn't associated with your Apple ID.

When downloaded, you'll need to goto *Disc Utility* to prepare the drive (HDD/SSD) - NOTE: if computer still has a HDD, it's HIGHLY recommended to change for a SSD as they're not damaged by movement, can be 10x quicker & as macOS is, by far, the slowest operating system, it'll HUGELY benefit from the greater speed) - (either create partition(s) or volume(s) or erase), connect to the internet either via LAN or WiFi & then can select *Install macOS*. It'll take a LONG time, far longer than the minutes 'estimated' on screen (unlike Windows & Linux which takes 5-10 minutes, macOS often takes MANY hours!), 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 (all correctly setup), keeping ALL installed software up-to-date & NOT using Google for searching, significantly reduces the risk of infections.

We install the following programs (if compatible with the computer & version of macOS installed (*Apple ID login details required):

***CornerStone Basic Software Suite*:** (from £39) - includes all available macOS updates

Avira◊: Block & remove viruses, malware, spyware, etc & firewall to stop attacks	**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	**LibreOffice**◊: Microsoft compatible word processor, spreadsheet, presentation, desktop publisher & database	**Mozilla Thunderbird**◊: secure email client with spell checker, anti-SPAM & anti-phishing
RustDesk: remote control of another computer - we offer support at £5 per 10 minutes	**iGlance**◊: display CPU temperature & CPU, RAM, disc + network usage & fan speed	**Foxit PDF reader**◊: Adobe Acrobat/PDF reader support all formats - fast, safe & compatible
250+ Solitaires*: huge selection of patience card games e.g. Klondike, Australian, Algerian, Duke		

updated: 20220821

***CornerStone Premium Software Suite*:** (from £49)

Skype◊: internet chat & reduced rate computer to telephone calls	**Microsoft Teams**◊: internet chat, voice & video & collaboration with large & small teams	**Zoom**◊: internet chat, voice & video & collaboration with large & small teams
VLC: media player with many built-in codecs for CD/DVD & audio/video files	**Commander One**: twin window file manager	**onyX**: maintenance, optimize & cleaner
Krita: image editing, similar to Adobe Photoshop or Corel Painter	**Send Anywhere**: allows sending/receiving files between Windows, Linux, Android, macOS & iOS	**Steam**◊: online gaming platform with 1000's of available titles

updated: 20220821

◊=requires setup (where applicable, we've already done!)

NOTE: Adobe Flash was discontinued on 31/12/2020 & blocked from 12/01/2021. Do NOT install Adobe Flash, Oracle Java or Adobe Acrobat (all unsafe). Acrobat/PDF support is included in Foxit (safer, faster & more compatible) & also in macOS & web browsers (which also include Java).

updated: 20220821

1. Things to do first:
   - read these notes (skip any not applicable), paying extra attention to yellow (important) & red (critical) highlighted ones! (there's a copy on the desktop & also 4 documents of police advice on how to spot & avoid various types of fraud & scams).
   - connect to internet - see #2 below (TAKE NOTE OF POTENTIAL ISP BLOCKING ISSUES AT END OF PARAGRAPH).
   - install all available updates.
   - install device drivers for any peripherals (e.g. printer) - see #10, #12 & #13 below.
   - install any other required software that isn't included in the *CornerStone Software Suite*. Be mindful you'll need to know your login details (generally an email address & password) for anything that's web based or requires activation. This isn't anything we could know, backup from previous installation or find out for you, so you'll need to know them! If it's just password you've forgotten, then it's common you can reset it via publisher's website.
   - copy back any data files from external drive(s).
   - start using computer… remember, you'll need to know your login details for email & websites as none are currently known to web browser(s), unless you previously signed into your browser & had sync enabled (obviously, you'll need to know the browser account details to sign-in again, which are usually email address or telephone number & password).

2. 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 or 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 (image varies for different versions of MacOS & desktop: signal bars, little screens or a globe are common, but it'll say "not connected", "connections available" or words to the effect, when you put the cursor over it) & 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 service provider (ISP) - 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, Edit/Network Connections, Advanced, select connection, click "-" to remove, Ok & 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 & see if supported - if not, you'll need to install device drivers (& maybe software) which might either have come on a CD or be stored on the modem. Once recognized, 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 or 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 completely & 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, Safari), 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.

Some ISPs (reported with BT/EE, TalkTalk, Sky & Post Office - rated by OFCOM & Which? as amongst the worst in the UK for reliability, speed, support & costs!) have started blocking secure internet connections, so they can continue to record your browsing habits (this is something they've been doing for years, but it's now possible to block them, so they've started blocking the blocking!) & use or sell the information (this is a serious privacy issue!). If connected to internet but you can't access ANY website, you might need to disable *DNS-over-HTTPS* (DoH: encrypts web address lookup to improve security & privacy) (common with TalkTalk, Sky & Post Office) or *Virtual Private Network* (VPN: routes internet connection through a different server to hide your actual 'IP address' (to block location tracking) or, if set to another country, for region bypass) (common with BT/EE). The VPN could be built-in to your web browser (e.g. Opera), be part of your anti-virus (e.g. Kaspersky) or could be a 3rd party program (e.g. OpenVPN). Most major web browsers have built-in DoH...

Opera:	*Menu, Settings, Advanced, Browser, System, Use DNS-over-HTTPS instead of the system's DNS settings*
Microsoft Edge:	*Menu, Settings, Privacy, Security*
Mozilla Firefox:	*Menu, Tools, Preferences, General, Network Settings, Settings, Enable DNS over HTTPS*)
Chromium based:	*{browser name}://flags/#dns-over-https* (replacing *{browser name}* as appropriate (e.g. chrome, etc))

...to protect against 'man-in-the-middle' attacks (where your intended website is redirected to another, that may look similar, but will record your login or payment details to use or sell) & can prevent access to known malicious websites (these often contain infections that can install without you clicking on anything (your browser should block these, as long as you have a popup blocker & an up-to-date advert blocker installed & they're both turned on & setup)), providing you with safer internet at no cost or effort to you, however, it's generally turned off by default! To enable, see above or browser website help or forums, but if your ISP doesn't support it (i.e. getting nothing but DNS errors), you'll need to disable it! Some ISPs 'piggyback' off another, so although your ISP may not restrict access, the actual service provider might. If you don't use a VPN or DoH, then it's likely your ISP WILL record & use or sell your data anyway! Many also record location, ethnicity, sex, sexual orientation, job status, marital status & much more with little or no control over how they use it! Targeted information has great value to advertisers & ISPs can make a lot of money from your data! The Domain Name Server (DNS) is basically a 'phone book for the internet' & it can be read by anyone, so DoH encrypts web addresses & includes them in standard HTTPS traffic, preventing recording or blocking. Although DoH adds an additional layer of protection & increases privacy, your browsing can still be inferred by ISPs (albeit in a reduced manner), so using in conjunction with a VPN is better. Until IPS are barred from 'stealing' your data, it's highly immoral, massively infringes on your privacy, limits your internet safety & removes any & all confidentiality, but you 'might' be able to use a VPN or DoH to block them. If you just get a blank webpage, with no error message, this is likely to be a *cookies* issue (see #3 below).

3. Many websites use 'cookies' to store your information & settings for their website (e.g. location for local news or weather)... this is literally just a text file & poses zero infection risk. However, more 'dubious' websites can use the cookies to track & record other information & usage habits, even from different websites, which they can then use for specific targeted content or advents or they can sell to 3rd party companies who build up a profile of your internet use. Companies like Facebook & Google may well have thousands of records on an individual (they are legally required to provide this information to you upon request) & they make a LOT of money by selling it. For privacy reasons, you would want at least 3rd party cookies (content not related to the main website you're browsing) blocked by default, which could be either all the time or just when the browser is in 'private mode' (this stores & tracks nothing, leaving no trace of the sites you've been to). However, whilst European law requires ALL websites to prompt for you permission to use cookies, some websites are now insisting you accept or you can't access the website. Some quite legitimate websites will use 3rd party companies to handle the cookies, meaning if blocked by the browser, you could be presented with a blank page even if you've selected 'customize' to see what information they want, so you can select which cookies you're willing to accept... in those cases, you'll either need to not use that website (recommended), or temporarily change your browser settings to not block cookies (change back again after exiting that website). For example, in Opera, goto *Settings, Privacy and security, Cookies and other site data, General settings*, select which cookies policy you want/need to use.

4. 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!

5. 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.

6. 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: *id* or *1234*. Files (e.g. documents, pictures, etc), like Windows & Linux, can have "read-only" permissions, preventing overwriting or changing... to change: select file, *Get Info*, tick/untick *Locked*.

7. 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 less likely to be compatible with newer software & newer versions of macOS are less likely to be compatible with older software) & you can just browse or search to install any program (click *Get/Install*)... 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). Apple released macOS 11 (Big Sur) in 2020 & macOS 12 (Monterey) in 2021... visually, the same as for nearly 20 years, nothing's changed, but the app store is almost empty (this should get better over time, but could take years!), implying they're not compatible with macOS 10... However, many macOS 10 programs can still be downloaded from the publisher's website & manually installed & they will work ok. If you can't find what you're looking for in the App Store, then it's worth trying this approach. Due to woefully inadequate cooling on Apple computers(!), there are MANY reports of the high CPU use during an upgrade causing the computer to overheat & die, with no option to repair other than replacing the motherboard (£500+!!!). It's HIGHLY recommended to install a program to monitor temperatures (e.g. iGlance, Hot, etc) so you know before trying if this will be an issue. However, the only realistic prevention is to disassemble computer (iMac are now glued together(!) - you'll need a hot-air gun to try to melt the bonds & run a high risk of breaking the glass or screen, so be VERY careful!), remove heatsink(s) & fan(s), clean them & vents & apply new thermal paste to chip(s) & then reassemble, all of which can be VERY time consuming, VERY awkward & fiddly work, but is still necessary to do as part of regular maintenance. Most Apple computers we see are dead due to overheating - it's a VERY common occurrence & due to Apple's extremely high prices, repair is rarely cost effective.

updated: 20220630

8. 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'.

9. 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* (winehq.org) & *PlayOnMac* (playonmac.com)... if not already present, install from App Store or publisher's websites. If a Windows based program is in the supported 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.

10. To add a printer: check if CD that came with printer supports your version of macOS (to limit incompatibility), else download & install the device driver(s) from manufacturer's website (e.g. epson.co.uk, canon.co.uk, etc) for updated drivers - this is good practise anyway to ensure the latest version is installed & required if you've mislaid the CD/DVD or your computer doesn't have an optical drive. When printing, make sure the indicated printer is the one you want to print to - most software 'remembers' the last selected output device - & look for *Print...* (often via *File* menu or by pressing *Ctrl+P*) rather than *Print* on menu as this displays the printer dialogue options allowing you to: 1. confirm the correct printer is selected, 2. select number of copies & which pages to print, 3. specify desired print settings (e.g. print resolution/quality, orientation, page size, etc). If items are unable to print (e.g. sending A3 document to A4 printer, which can't work, so blocks print queue for everything sent afterwards), then cancel items in the print queue from last to first, else you could get multiple copies printing of items sent after the first. It's very rare for websites to have a print option (email being an obvious exception), so when selecting print from browser menu, unless it (e.g. Maxthon) supports *reader mode* (removes all extraneous content), then browser has no way to know which part(s) to print, so you'll get everything on the page: text, pictures, menus, adverts, etc
When fitting ink cartridges, it's common they will have a plastic 'tab/tape/cover', stuck on one edge, that MUST be removed first (there might also be a clip support to remove). It covers an air vent & MUST be removed to allow ink to exit the cartridge (imagine holding your finger over a straw that's full of water - the water can't come out until you uncover the top, releasing the vacuum seal). Failure to do this could literally burn out the nozzle for that colour, meaning it'll never be able to print properly again! Also, when inserting, make sure the cartridge 'clicks in' ok, else it won't be detected. For Canon inks, if the light doesn't come on when inserted, place the plastic tab in front of the clip & this 'tricks' the printer into seeing the cartridge (it might inhibit ink level monitoring, so pay attention to indicators & how printing looks)! Some printers warn when inks are low, encouraging you to change them, but if that colour is still printing ok, it's NOT yet empty, so ignore until it starts to fade/break up & you'll get more printing per cartridge.

11. Since most infections are web based, a safe web browser, correctly setup, is absolutely CRITICAL to limit attacks. We recommend, install (if compatible with computer & version of macOS) & setup Opera. Opera 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), DNS-over-HTTPS website 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). Whilst you may use whatever browser you wish, try to avoid Apple's Safari, Google Chrome (not technically a web browser, but a spyware infection, sitting on top Chromium browser, recording & selling your data!) & Mozilla Firefox – all are slow, unsafe, incompatible & have very few features. In addition, internet security will NOT protect you from web browser infections! There are MANY browsers based on Chromium (e.g. Opera, Maxthon 6, Chrome, Vivaldi, Brave, Microsoft Edge (new version), etc… So if a website works in one, it should be no different in another. **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 won't lose them when hard disc drive or solid state drive fails or macOS is reinstalled! Anything entered into the address bar, which isn't in the format of a web address (i.e. site.domin{.sub-domain}), is deemed to be a search. For example, *bbc.co.uk* (exists) & *bbc.abc* (doesn't exist) are both in the right format, so both would be checked for accessibility & displayed, if available, whereas *bbc* isn't in the right format, so would be searched for instead. When you don't know a web address, type what you do know to help find it (e.g. *bbc* will show *bbc.co.uk* in the search results, but so too would *news*). We set the default search engine to DuckDuckGo, - they are privacy oriented & don't record or track anything, but have optional search filters for where (country) & when (last day, week, month, 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 uses Yahoo, but is pre-filtered to show less. Yahoo has been bought by Oath, who keep informing you Yahoo is now part of their services whenever you search, so quickly becomes annoying! If a webpage is displayed with writing too small or big to read, pressing *Ctrl +/-* zooms in/out & is 'remembered' per website, so the next time you go back to the same webpage, it'll have the same zoom settings.

updated: 20220512

12. Unlike Linux, macOS has very 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 to install device drivers (check manufacturer's website). Also, not everything is compatible, so older hardware is less likely to be compatible with newer versions of macOS & older macOS is less likely to be compatible with newer hardware.

13. 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 printers: is there ink in the cartridges & are they correctly inserted, is there paper in the tray, is there anything blocking paper input/output, is there anything stuck in the print queue (e.g. A3 document sent to A4 printer can't print thus blocks everything after- delete entries from last to first if multiple copies sent). 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! Corrupted settings in the *System Management Controller* can prevent hardware detection or affect function, to reset: shutdown, hold *Shift* + *Control* + *Option* keys & press *Power* key & keep holding them for 10-15 seconds, then release & power on normally. If hardware isn't initiating properly then could be corrupted firmware values held in *PRAM*, to reset: restart, hold *Command* + *Option* + *P* + *R* keys & wait for second chime (if no chime(s), hold for 10-15 seconds then release) while booting.

updated: 20220512

14. 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, but NOT within the first week of any major update as they often screw it up with glaring bugs/issues (let someone else be the beta tester!). Updates can fix security issues, add new features or improve existing ones, but, unlike Windows updates, like Linux, macOS updates also include all programs installed from the App Store!

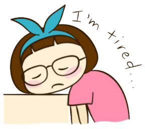
updated: 20220630

15. 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 (they're case sensitive, so "abc" is NOT the same as "aBc" - try swapping case & trying again), via a web browser, goto the email service website (e.g. outlook.com, bt.com, 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 (client) 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, not just computers, will read 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 use an email client (e.g. Microsoft Office Outlook, Thunderbird, etc) you will need to reinstall the email program, re-enter your email account details (e.g. email address, password, inbound/outbound mail servers, etc) & then import the email & contacts from the backup folder. Apple's *Mail* program is unsafe, so should be avoided, however, if you were previously signed in with an Apple ID, then it will likely have stored the account/login details for you (except maybe password) & you'd not need to know or enter them again! Most internet providers include help on their website on how to do this. Ideally, always use a webmail email provider (e.g. *outlook.com*), NEVER anything from your internet service provider (e.g. BT, TalkTalk, etc) so when you change ISP, you don't lose your email address (e.g. yourname@talktalk.net) & you can access your emails from any internet connected computer, tablet, smart phone, etc. Webmail never needs to be backed up, you can access it from anywhere on the world & you can't get infected from malicious attachments unless you manually download & open them! If you have used an email address from your ISP, changing all the websites & services you've previously signed up for could be VERY time consuming (assuming you even known them all!?) & for some ISPs, you'll actually need to pay them (often £8 per month!) to keep the account active (at least until you've changed everything). If you have pre-printed business cards, stationery, etc, then you'll probably want to use that up before making changes. Using ISP email can become quite costly when you later realize you made the mistake. For SPAM email, NEVER unsubscribe else you've confirmed address is 'live' & you'll get far more & malicious emails!

There's a common mis-understanding about email, in which people think email is being sent to them or their device(s) (i.e. computer, telephone, tablet, etc)... This is a critically important & fundamental error as email is NEVER sent to people or their devices, it is ONLY sent to the email service provider (e.g. yahoo.co.uk) & 'you' can then look at (via a web browser) or download (via an email program (client)). If you have an email client (e.g. Microsoft Office Outlook, Mozilla Thunderbird, Apple Mail (unsafe), etc) that's setup to check, for example, every few minutes & the device is connected to the internet, then it can alert you when new emails arrive. But, if it's not setup to check or the device is not connected to the internet, then obviously it can't tell you! If you view email on a website (e.g. yahoo.co.uk) in a web browser (e.g. Opera, Safari, Chrome, etc), then again, if you're not running the browser, with that page displayed, or the device is not connected to the internet, then you'll not know about any new emails. It's irrelevant how often you check, look or not as the email address will still be able to receive emails, you just won't know about them until you're next able to check. There's one exception, that will prevent any new emails getting through & that's if your email mailbox is full... this is uncommon these days as most email providers allocate quite a large amount of space, generally enough for many year's worth of emails. Additionally, however you access emails, any attachments don't exist as usable files on your device until they're downloaded or saved from the email, selecting a folder to store them in & optionally giving/changing a filename. If you need access to previous emails, even when not connected to the internet, then you'll need to use an email client & the recommended choice for safety, speed, features, ease of use & compatibility, is Mozilla's Thunderbird (available for Windows, Linux & macOS).

Understanding Email

16. If possible, try to position your computer screen at or above eye level as holding your head up, rather than looking down, causes the body to release norepinephrine (a chemical messenger from your central nervous system & a stress hormone released from adrenal glands) to keep you in a wakeful/alert state. If you feel tired, your eyes start to close & your chin drops, but physically just tilting your head back & looking up for 10-15 seconds triggers the brain to put you into an alert state! However, you should take rest breaks every few hours anyway.



updated: 20220818

17. 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. Samsung, Apple, Nikon, etc) 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 male (plug) to B male. Extension leads are generally USB A male (plug) to A female (socket). Computers generally have USB A or C sockets, which, without a separate convertor, don't carry video & two computers can't be linked together. Black USB sockets are generally USB2.0 (unless "SS" (super speed) then USB3.x) & blue are USB3.x, which are MUCH faster. Other colours generally mean higher power output (standard is 0.5amps, so could be 1.0amps or more). Try to reserve the faster sockets for devices that will benefit (e.g. USB HDD/flash).

18. 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).

19. It's common, websites or emails will have *Portable Document Format* (PDF) files & state you need *Adobe Acrobat* to open or read them… this is NOT correct! You do need a PDF reader & although Acrobat is indeed a PDF reader, it's slow, unsafe & incompatible - you'll find some PDF files can't be opened & some can't be printed - so it's NOT popular or recommended. For many years, the preferred PDF reader is *FoxIt Reader*, which is faster, safer & more compatible. If we've (re)installed macOS, you'll already have *FoxIt Reader*.

updated: 20220819

20. To photocopy something, you need a scanner & a printer & it's common nowadays these are combined into one unit. Most often, you can just lift the scanner lid, place the item on the scanner (make sure to line it up), put the lid down & then press either the black & white or colour scan button & it'll do the job. However, if you want to scan a picture or document into macOS (e.g. to store, edit, email, etc), then you need to use software. For any program that supports import via scanner, when selected, it'll run the scanner's own software (which generally can't be run on it's own). You can select settings such as: *Type* (e.g. document, picture, etc), *Resolution* (measured as Dots Per Inch (DPI) - higher is better quality, but bigger file size & *Colour*, *Grey Scale* or *Line Art* (just black or white, no shades). Click *Preview* for a quick check to see if you've lined it up ok & then *Scan*. After completion, the image (everything scanned is a picture) will be passed back to the program that initiated the scan, where it can be saved (in any format supported by that program) or edited (if, for example, a photo editor), leaving you ready to remove that item from the scanner & put the next one in to *Preview* & *Scan*.

updated: 20220630

21. 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).

22. 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 (this is known as a 'filter bubble') to show the results they can make the most advertising revenue from! They prioritise results to show their own companies or services first, then others with adverts & eventually, whatever is left that matches your profile. Of the top 1 million websites, 75% have Google tracking embedded to record & sell your data! Another person, using exactly the same search criteria on Google, even at exactly the same time & even in private/incognito mode, can be presented with wildly different results as they're based on that person's filter bubble! For example, one's browsing & search history for medical, political, religious, etc matters are likely to only show what you want & expect to see as that's what your profile contains, so you won't see any opposing views or the other side of an argument. Also, people against (for example) vaccines, will see results supporting their beliefs & people for vaccines will see the opposite, in both cases reinforcing their beliefs, 'proving' they're both right! Do exactly the same search on Yahoo, Bing (both filter, but not to the extent Google does) & DuckDuckGo (ZERO filtering) & you'll find substantially more applicable hits, which are also far safer (less scams) & you'll be better informed! Since DuckDuckGo record & track nothing (so every search is a 'first' search), have options for selectable country, can omit adult sites & search by date/time, they are the recommended choice (privacy first!). Much of the information on the internet is either wrong (e.g. there's lots of conspiracy theories & 'fake news') or out-of-date (therefore, technically, still wrong!), so finding current & accurate information is made much easier with DuckDuckGo!

23. 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's 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! File names are in two parts, name & extension, separated by a dot/period (e.g. letter.doc). macOS keeps a list of file extensions & the programs associated with them (e.g. ".doc" might be linked to LibreOffice Writer, Microsoft Word, or whichever word processor you have installed (if any). Changing or removing the file extension will prevent macOS correctly identifying the type & so it wouldn't be able open the file! When editing existing files, it's good practice, BEFORE making any changes, to click *File*, *Save As* & give it a new name (e.g. letter.doc to letter1.doc) & then any changes you make won't affect the original file, meaning you can go back if need be. Documents & pictures tend to be small files, so you won't be wasting lots of disc space! Like in Windows & Linux, user folders (e.g. documents, pictures, music, videos, etc) are stored in the *user* folder.

updated: 20220819

24. The world's greatest internet threat is the rise of ransomware infections – these encrypt all your data files & then demand £100's (sometimes £1,000's & for corporations, often £1,000,000's!) payment within a short time to decrypt them else they are permanently lost or released/sold on the internet! They are mostly distributed by email & malicious websites (often accessed by Google 'search' or malvertising (fake adverts)). **ALWAYS backup important files & make sure ALL installed software is kept up-to-date.**

25. 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.

updated: 20220512

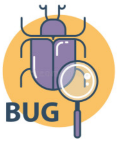
26. When signing into a website (e.g. email, banking, shopping, etc), if website says email address or password are incorrect, this means, however sure you were that you'd typed them correctly, you've typed one of them wrong! Although email isn't case sensitive (e.g. FredAndGinger@hotmail.co.uk is ok), 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) or via security questions you previously setup/selected, 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 it's fine to use the same, easy-to-remember password, for any non-critical websites (not email, financial or social) & then secure/long just for those that warrant it. For websites/services that support it (e.g. common for many email, banking, shopping, social media, etc), it's a good idea to enable 2 factor authentication (2FA, generally requires you enter a code sent to your mobile phone) & this way, even if criminals know your email address AND password for a service, they still can't login or access your emails/files/etc.

updated: 20220512

27. 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 cyber criminals & scammers. To reduce the chances of getting infected or being conned/scammed, follow one simple rule: if something doesn't look right, or it just seems suspicious, then it most likely isn't safe, so don't click on it!

update: 20220512

28. Most software contains 'bugs' - errors in the code due to poor programming or inadequate testing (Apple, Google & Microsoft are all bug experts, creating many of them!) - however, a badly written program can have what's known as a 'memory leak', where it overwrites memory contents belonging to other programs, so identifying the culprit is not always obvious as errors could be caused by a completely different program. Keeping ALL installed software up-to-date will limit the impact of bugs, but initial releases (e.g. v1.0) of new programs should be avoided until the first point release (e.g. v1.1).



updated: 20220512

29. We've had a lot of customers tell us they've had a message on screen telling them they're infected & asking them to call a 'support' number who try to sell them a bogus support contract! Similarly, customers who've been called, often saying it's Microsoft, Apple 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. Another common scam is sent via email, claiming they have incriminating evidence against you (for something you haven't done!) or saying they've 'hacked' your computer or router & downloaded your data & threaten to send it to people in your address book! The pre-internet letter claiming a Nigerian millionaire had died & if you allow them to transfer his money to your bank account, so the government can't take it, you'd get a commission, is now arriving as an email - often containing deliberate spelling mistakes as the people who don't notice must be of lower intellect(!) & so are more likely to fall for offer! They're all just scams that often costs £100's or even £1000's! If you've already been a victim of any of these scams, contact the police & report it to your bank – you've been robbed! If something looks or sounds too good to be true, then it probably isn't!

30. Crypto-currency coin mining is basically using your computer to run a 'mining' program to process calculations for someone else, for which you'll earn a (very) small amount of money. If you have a (ideally many) super-fast computer, you can do more calculations & so earn more money... but it's rarely cost effective once you factor in cost of the hardware & increased electricity costs. However, if you notice your computer is running slow & *Activity Monitor* shows an unrecognized process consuming a lot of CPU time, you might be infected with a uninvited mining program! Here, you're losing performance & paying for the electricity, but you're not receiving any money! Run scans with multiple anti-malware scanners to get the best chance of removal.

updated: 20220512

31. 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

32. 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.

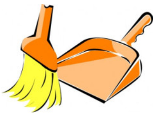
33. Whichever office suite you install/use (e.g. LibreOffice, Microsoft Office (via Wine), WPS Office, etc), they all share, to varying degrees, common layout (generally configurable & some support different 'themes'), functions & short-cut keys, so mostly, the way you do something in one is very similar (or exactly the same!) as another. Menus often show the short-cut keys next to an option & if you learn these, over time you'll find that's much quicker than using just the mouse, menus or icons:

To highlight text, use either mouse with left button held or shift+cursor keys (optionally with Home (beginning of line), End (end of line), PageUp (previous page), PageDown (next page), Ctrl+Home (to start of document), Ctrl+End (to end of document)

key	function	why that key
Ctrl+A	to select all text	first letter of ALL
Ctrl+C	to mark a highlighted area for copying	first letter of COPY
Ctrl+X	to mark a highlighted area for cutting/moving	X looks like scissors (cut)!
Ctrl+V	to paste a marked area for copying or moving	next key on keyboard!
Ctrl+L	justifies text to the left (current paragraph or highlighted text)	first letter of LEFT
Ctrl+R	justifies text to the right (current paragraph or highlighted text)	first letter of RIGHT
Ctrl+E	centre align text (current paragraph or highlighted text)	last letter of CENTRE
Ctrl+J	left & right justifies text (like in books) (current paragraph or highlighted text)	first letter of JUSTIFY
Ctrl+B	toggle bold on/off	first letter of BOLD
Ctrl+I	toggle italics on/off	first letter of ITALICS
Ctrl+U	togges underline on/off	first letter of UNDERLINE
Ctrl+S	save document - if already has a filename, else prompt first for filename	first letter of SAVE
Ctrl+Z	undo the last change - this can often undo back to start of creating/editing file	first letter of ZAP!
Ctrl+Y	redo last undone change - this can redo back to last change made	previous letter in alphabet to Z!
Ctrl+P	print dialogue box to check correct printer selected & specify copies, which pages, etc	first letter of PRINT
Ctrl+F	find - to locate next occurrence of entered text	first letter of FIND
Ctrl+G	goto (move cursor) to specified page/line/paragraph/etc	first letter of GOTO
Ctrl+H	find & optionally replace next occurrence of entered text	next key on keyboard!
Ctrl+O	open dialogue box to browse drive(s) & folder(s) to locate file to edit	first letter of OPEN
Ctrl+W	close current document/window - if unsaved changes, prompts first to save or cancel	first letter of WINDOW

updated: 20220630

34. 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 (at least once a year) for dust build up & clean when necessary. Thermal paste (between chip(s) & heatsink) should be replaced if dried out. For PCs, do NOT put them on carpet (unless office/short pile) as that's where dust, dirt, hairs, etc collect & you'll be blocking PSU air intake (now commonly at bottom of modern PCs) causing it to overheat or become less stable. Better to place PC on a (e.g. wooden board) flat surface. Make sure the case has good air flow (dependant on specification of components as 'high-end' CPU & graphics or more drives will generate more heat) - fan(s) at front bringing in fresh air & at back removing & if space available, ideally side fan(s) blowing in & top extracting) else the CPU, graphics & even some SSDs will be throttled to keep cooler, losing performance! Modern Apple All-In-One PCs are glued together, so removing the screen is difficult, risks breakage & will need to be re-glued after cleaning, meaning it's safer to get that done professionally! If portable computers have air vents on base then they MUST be used on a flat surface to limit overheating (NOTE: Apple portables have no air vents on base, so overheat easily &, if not cleaned regularly, will easily burn out & die!). If they contain mechanical/hard disc (rather than solid state) drive(s), then they MUST be used on a steady surface to limit drive damage - movement, while powered, causes drive heads to hit disc surface (think of them like a record player), damaging disc! It could stop booting up or you could lose files! Air vents or HDD mean they're a 'notebook' NOT 'laptop' & MUST be used accordingly (it's irrelevant what you call them, but it matters how you use them!). Since batteries are for portable use, after charging (ideally, not more than 80% & don't let 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! Most modern portable computers have the battery on the inside, so can't easily be removed (& may not work if it was or would lose settings (e.g. date, time, etc)), meaning it'll constantly be killing it, reducing it's capacity! macOS only reports charge level & 100% of nothing, is still nothing! If removing battery, put it back in to top it up every few months to keep it 'alive'.



35. 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 (HDD) & solid state drives (SSD) fail - no exceptions - & infections/attacks can corrupt files! Make copies on external hard disc, USB flash drives or online storage, but, ideally, not optical (e.g. CD, DVD, BD, etc) discs (short life span & unreliable). DropBox (2GB free) or Microsoft's OneDrive (5GB free) are both recommended online backup options, but you'll need to pay if you need more storage space. Due to the potential for a ransomware infection to encrypt any & all files it can access, it's CRITICAL to NOT leave your backup media (i.e. USB flash or external drive) permanently connected, else that too will be encrypted & ALL your data lost! Only connect the backup drive as & when needed & eject (click icon (looks like a USB plug with a green circle & white tick) by clock to safely finish writing any updates stored in the cache) & remove after use.

updated: 20220512

36. CornerStone Computer Centre sell inkjet cartridges & laser toner at the lowest prices (by far!) in the area. We keep large stocks of Epson, Brother, Canon & HP individual inkjet 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 to buy than individual inks (commonly £2-£4), they put a lot less ink in them & losing 2/3 when only out of 1 colour means the effective cost per page can be 100-400x more expensive! NEVER buy a two cartridge inkjet printer &, if you already have one, when the inks run out, just buy a new printer (see our website for printer recommendations) as it'll save you a LOT of money on the running costs!

updated: 20220512

37. For most people's computer usage (i.e. internet, email, typing, pictures, music, videos, etc), they would be far better off to use Linux instead of Windows or macOS! Linux is MUCH faster & safer, looks & is used in basically the same way & is FREE! There are over 300 versions available, but for speed, ease or use, compatibility & features, we recommend Manjaro & Linux Mint (both with 'MATE' desktop & 'Blue Submarine' theme) & charge from £29 to install with the Linux equivalents of our software suites.

updated: 20220512

Our 'Hints & Tips' guide contains a list of common 'good' (safe, fast or functional) & 'bad' (unsafe, slow or basic) software (mostly for Windows, but macOS too)... get it, together with price guides & servicing details via our website: http://www.CornerStone.me.uk

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

If you have any suggestions, find any errors, paragraphs you thought weren't clearly explained or even topics that aren't covered but you think people would benefit knowing about, please feel free to send your suggestions to: feedback@CornerStone.me.uk