



BYOD Laptop Program – Connection Checklist

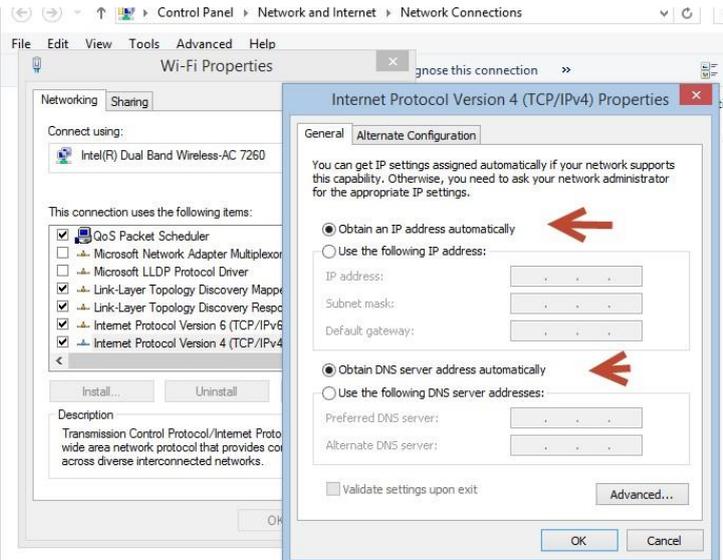
This document is a checklist for parents and students to action prior to bringing a BYO device for connection to the DET (Department of Education and Training) BYOD network which is available at Cavendish Road State High School.

Please check each item, contact the HOD Information Services with any questions. Contact details are at the bottom of the document. There are many checks required to ensure that the school is able to provide the BYOD connection process (called onboarding) for a wide range of devices.

CHECKLIST

1.	Laptop must meet specifications. Our specifications for BYOD devices are published on our website at this link . Chromebooks, Linux devices and Windows XP ARE NOT supported by the DET BYOD network. Windows installations should be 64 bit as much of the Adobe suite used by the school will not run on 32 bit windows.	
2.	Laptop must have a login screen and not boot straight to a desktop The DET method of connecting to wireless adds a security certificate which is unique to the student linked to both their school username and the user they are logged into on their device. If there is no login, the certificate cannot be created.	
3.	Student MUST be an administrator (not temporary) of the laptop The student must have an administrator account on the laptop. This cannot be a temporary account. The DET BYOD system will not work with non-admin accounts.	
4.	Personal firewalls (this is different to anti-virus) should be turned off while at school Many devices have personal software firewalls. These prevent connections and interactions to safeguard the computer. Some of these firewalls interpret the DET BYOD network as hostile and block access to the DET servers. NOTE: Firewalls and Anti-Virus do different things. Firewalls are concerned with network traffic and blocking hostile traffic. Anti-Virus is concerned with preventing “Malware” (Malicious Software) from running on the computer. Many Security products bundle these two functions together, but the control panel will allow the user to turn off parts of the security.	
5.	Laptop must be set for local time and locale. Brisbane, GMT+10 (no daylight savings). Enterprise networks like the state-wide DET network use time and date as critical parts of the security system. If the date and time is wrong, the laptop will be unable to connect. The correct	



	<p>time zone should be set (make sure it is BRISBANE to avoid Daylight Savings Time) as well as the correct date and time.</p>	
<p>6.</p>	<p>Date and time must be accurate to within one minute of school servers.</p> <p>Setting the time to within one minute of that on your smartphone is acceptable. Your smartphone gets date and time using the same method as the school file servers. Laptop that are even 5 minutes out will not connect.</p>	
<p>7.</p>	<p>Geo location software will prevent connection.</p> <p>Geo location software is sometimes used to make a device pretend to be in another country. One common reason for this is to access services that are blocked outside that country such as television/movie streaming services. Geo Location software should be removed from the device.</p>	
<p>8.</p>	<p>Language must be set to English (US, Australia or UK)</p> <p>Language must be set to English for connection. It can be set to other languages after that but please consider that in class, your teachers need to be able to read the screen in order to assist you with your work. Ensure you have an English language pack installed and switched on when you come to on-board. These can be downloaded from Microsoft or Apple.</p>	
<p>9.</p>	<p>The WIFI should be managed directly by the operating system.</p> <p>Some laptops have “WIFI Managers” installed or are even sold with them. This software sits between the operating system and the WIFI card and may prevent connection or make the connection unstable.</p>	
<p>10.</p>	<p>There must be no static IP or DNS settings on the wireless network adaptor</p>  <p>Some users set these for home networks, or for DNS to 8.8.8.8 (Google DNS). Both of these will prevent the device from connecting. The wireless NIC must be set to get all settings automatically. A screen shot of the relevant windows dialog with the correct settings can be found in the above screen shot.</p>	



CAVENDISH ROAD *State High School*

11.	There must be no pre-installed proxy settings on the wireless network adaptor Proxies should not be manually set. This will prevent access to the DET servers.	
12.	No VPN's are to be installed on the device, this may prevent proper installation of wireless certificates If VPN's (Virtual Private Networks) are installed, this can prevent connection of the laptop. This is also a breach of our ICT Policy.	
13.	Only 1 laptop per student is to be connected to the BYOD network. Please ensure that this device has all current updates prior to bringing it to school.	

Karen McFarlane HOD Information Services

kmcfa19@eq.edu.au Ph: 3394 0718