

Using_Non_School_Owned_Computers_on_MCC's_Network

In order to maintain network integrity and security, non-district owned computers must meet the following requirements in order to be allowed access to MCC's network resources. The computer must be brought in to Technology Support Services to be inspected for compliance with these guidelines. Please contact Technology Support Services at 480-461-7217 or tss@mccmail.maricopa.edu in order to make an appointment for this service. Wired network access is only granted to Faculty and Staff. **Wireless network access** is available to anyone with a **MyMCC** portal account, including students.

- The owner of the computer must provide their own Ethernet card. Some machines have this feature built-in. All Ethernet cards have a unique identifier associated with them ? this is called a MAC address or Ethernet address. This address must be registered in our DHCP server in order to provide you with network access.
- The owner of the computer will be responsible for any and all network traffic generated by that computer. Unauthorized or undesirable usage (such as viruses or Peer to Peer file sharing) will result in removal of network access from that computer. The owner must abide by **MCCCD's Computing Resource Standards**.
- A virus scanner must be installed and updated to the most current virus definitions. MCC has a site license for Symantec Antivirus that Faculty (including adjunct) and Staff can install on their home/personally owned computers. **Contact Technology Support Services** for more information on obtaining Symantec Antivirus.
- The operating system must be updated with the latest security patches available. Windows users can obtain updates by visiting **Microsoft's Windows Update website** with the Internet Explorer browser (Please note that Windows Update will not work with browsers other than Internet Explorer.) Macintosh users can obtain updates by using the Software Update feature in OS X.
- Windows users must also have a firewall in place. The built-in firewall in Windows XP is adequate for this purpose.
- The computer must not have any Peer to Peer file sharing programs on it such as Kazaa, Morpheus, Spinner, LimeWire, BearShare, or many others. For more information on this district-wide policy, please visit **this web page**.
- The computer must not have any unrestricted shares set up on it. We would prefer that the computer have file sharing disabled entirely.
- The network connection must be used for MCCCD related business only. However, in order to maintain network security, we will allow users to use the network connection to download security updates and virus scanner updates.
- If the personally-owned computer is ever sold or otherwise removed from the owner's possession, we must be notified as soon as possible so that we may remove the ability of that computer to access MCC's network. This is for your protection as well as MCC's.
- Please be sure to check individual policies for plugging in to the network at different facilities around campus. Some common areas and labs do not allow faculty and staff to plug their own computers into their network jacks.