JEFF TECH

Wireless BYOD and Guest Access Information

Jeff Tech can/will provide access to the Internet on personally owned instructors, staff, administrator and student devices (Phones, Tablets, Laptops, iPads, etc).

Please note, access to the JT-BYOD-WiFi and JT_Guest-WiFI will still be filtered for content per Federal Government's CIPA requirements.

Access Certificate

Note: The first time you access the JT-BYOD-WiFi or JT-Guest-WiFi network on a new device, come back to this same spot on JeffTech.info (High School – Public Forms & Documents – Information Documents & Links) and click on the "Wireless Access Cert Install"- follow the instructions in that document to install the "Sonicwall Access Certificate". After that point, and in the future, you can just start using the Internet on that device. Connecting to either network infers your acceptance of the **WiFi Acceptable Use Policy** defined below.

JT-BYOD-WiFi Info and Connection

Access to the "JT-BYOD-WiFi" is granted to all staff and Practical Nursing students automatically if they have a Jeff Tech Network user name and password. . Students can be granted access to the JT-BYOD-WiFi by request and if deemed necessary by administration. Students are NEVER given access to the JT-Guest-WiFi network.

To connect a personal device to wireless access, use your devices WiFi access methods to select the "JT-BYOD-WiFi" network. For most devices (Windows, Apple), when prompted you only need to enter your Jeff Tech network username and network password to access the network.

On newer Android devices, you may be prompted for more information: Use the following:

EAP Method: Select "PEAP"

Phase 2 authentication: Select "None"

CA certificate: Select "None" *(Note: you will get message that the connection is not private. This is normal and of no concern)*

Identity: Enter your network username

Anonymous Identity: Leave blank

Password: enter your network password

JT-Guest-WiFi Info and Connection

Access to the Internet for others without network accounts will be granted via the JT-Guest-WiFi network. Those users need to contact the IT Director or IT Technician for access passwords.

To connect a personal device to wireless access, use your devices WiFi access methods to select the “JT-Guest-WiFi” network. When prompted, you only need to enter the special access password provided by the IT staff to access the network.

WiFi Acceptable Use Policy

This Policy is a guide to the acceptable use of the Jeff Tech Guest and BYOD Wireless network facilities and services. Any individual connected to the Guest or BYOD Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

JEFF TECH MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST OR BYOD WIRELESS NETWORKS, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST OR BYOD WIRELESS NETWORKS YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS JEFF TECH FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.

Jeff Tech takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest or BYOD Wireless Networks.

Jeff Tech reserves the right to disconnect any user at any time and for any reason. The Guest and BYOD Wireless Networks are provided as a courtesy to allow our guests, employees and students access to the internet. Users will not be given access to the Jeff Tech intranet or permission to install any software on our computers.

Inappropriate use of the Guest or BYPD Wireless Networks is not permitted. This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that Jeff Tech may at any time use to make a determination that a particular use is inappropriate:

- Users must respect the privacy and intellectual property rights of others.
- Users must respect the integrity of our network and any other public or private computing and network systems.
- Use of the Guest or BYOD Wireless Network for malicious, fraudulent, or misrepresentative purposes is prohibited.
- The Guest or BYOD Wireless Network may not be used in a manner that precludes or hampers other users access to the Guest or BYOD Wireless Network or other any other networks.
- Nothing may be installed or used that modifies, disrupts, or interferes in any way with service for any user, host, or network.
- As defined by the US Government CIPA requirements, the Guest and BYOD Wireless Networks are both filtered for content, with the BYOD network being the most restricted. You are prohibited from doing anything that would circumvent the content filter. Doing so will result in loss of access privileges.