



Information Technology Services

Student Wireless Network Access

Purpose: The GCSC WIFI network will work with most personal wireless devices. This document demonstrates the use of Windows built-in wireless software. Your computer software may vary slightly in set-up. Your wireless device must support WPA encryption.

1. Depending on your operating system and your software configuration, you may see a message that informs you that you are within range of a wireless access point (see Figure 1). Open your wireless access software to enter your wireless setup. On some devices you will need to go to settings and then to Wi-Fi setup.

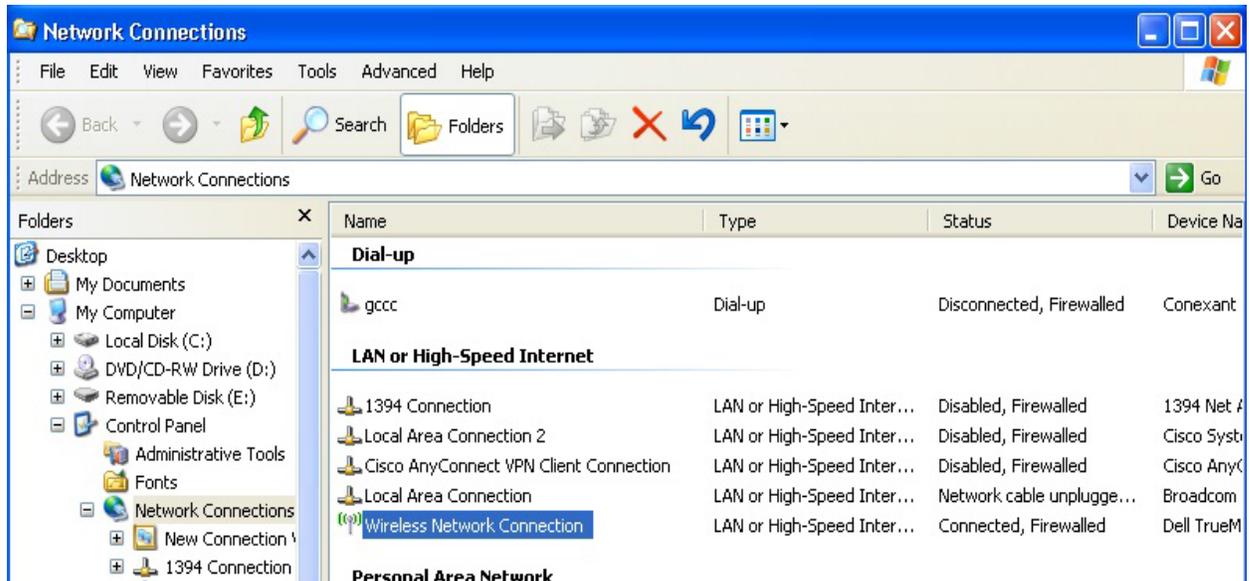


Figure 1

2. Ensure that the wireless access point you are choosing is a GCSC wireless access point. Locate and click the “gulfoast” wireless network to connect. (Figure 2). If you cannot see the network you may need to refresh network list”.



Figure 2

3. (Figure 3) When the Wireless Network Connection screen appears, enter the WPA2 network key gcscgcsc and click connect.



Figure 3

4. Navigate to any web page using your web browser. Logon using your MyGCSC user ID and password then click the Log In button. For local patrons: Use the username and password you received by email after submitting a wireless request.

REGISTERED USER

USERNAME

PASSWORD

Logging in as a registered user indicates you have read and accepted the [Acceptable Use Policy](#).

For Students:

- Use your MyGCSC user name and password to log on.

For Community Patrons:

- Use the username and password provided to you by email from the help desk.
- If you have not applied for a GCSC wireless account you can download and complete the [Wireless Access Authorization Form](#) to request free wireless access.

5. When your log in is accepted you will be redirected to the Wireless student portal page. This page contains the GCSC acceptable use policy.

6. Click accept to gain wireless web access to the internet.

Wireless Acceptable Use Policy

For your protection, sites visited on GCSC's wireless network are being monitored. Continued usage of this system and your signature on this access request form constitutes awareness and acceptance of this fact. When using the wireless network, you agree to refrain from the following:

- using the campus network resources for any illegal activity
- violating the conditions of those codes relating to student rights to privacy
- using profanity, obscenity, or other offensive language
- deliberately displaying obscene pictures or text on the monitor or allowing such images or text to be printed on the institution's printer
- copying commercial software or other commercial materials (including music and movie files) protected by copyright law
- using the institution's network resources for financial gain
- engaging in activities designed to deliberately obstruct others' work
- excessively using available network resources
- deliberately causing a machine to crash
- attempting to gain access to areas of any system for which authorized access has not been granted, i.e. 'hacking'
- engaging in activities that give simulated sign-off messages, public announcements, or other fraudulent system responses
- engaging in activities that do not have academic merit, such as: storing files not related to academic activities, using peer-to-peer file sharing software and/or deliberately executing files that excessively utilize the system
- giving away your user ID and/or password for any reason under any circumstance
- fraudulently using someone else's ID or password
- having or attempting to change system control information, such as program status, protection codes, and accounting information
- sending others material and then requesting them to send additional messages to others, i.e. chain letters
- sending bulk 'spam' email or intentionally utilizing system resources to send such messages
- unauthorized installation of any drivers, software, or hardware on campus computers
- using the institution's network to launch denial-of-service attacks against any computer or network

Violation of these policies can and will result in disciplinary action and/or prosecution. You are responsible for all activity that occurs on your user account. Gulf Coast State College and its employees disclaim any responsibility for anything that happens to your personal hardware and/or software while using our services.

ACCEPT

Note: Never share your username or password with anyone or allow anyone to use your connection. You are responsible for anything done using your account. If you have any questions regarding the usage or setup of your account, please call 769-1551, extension 3303.