Limestone Network (For Students/Employees)

1. Select the "Limestone" Wi-Fi network on your tablet, smartphone or laptop.
2. When your device prompts you, enter your Limestone username (the username is what is before the @ of your Limestone email address) and your Limestone password and click 'join' or 'ok'.
3. You will then be connected to the Limestone Network. This connection will be valid until your password changes.

iPhone/iPad

1. Select the "Limestone" WiFi network on your phone or tablet.
2. When your device prompts you, enter your Limestone username/password and click 'join' or 'ok'.
3. The next screen will ask you to accept a "Certificate" for clearpass.limestone.edu, Select "accept/trust".
4. You will then be connected to the Limestone Network. This connection will be valid until your password changes.

*If you experience issues connecting, Click **"Forget the Network"** and reconnect again following the instructions above.

Android Instructions

1. Turn on WiFi and select the "Limestone" network.
2. Be sure EAP method is set to PEAP.
3. Type in your username (same username used for e-mail and Canvas login. Do not include the @limestone.edu) in the field labeled "identity".
4. Type in the password in the "password" field (same password used for e-mail and Canvas logins)
5. If you are prompted for a certificate, choose default.
6. Click "connect"

Public WI-FI instructions

1. Select the "Limestone-Guest" Wi-Fi network on your device.
2. On your tablet, smartphone or laptop.
3. Open a web browser (Safari, Chrome, IE, etc.) and browse to any new web page.
4. You will be redirected to the Terms of Service page
5. Check the box to accept the Terms of Service.
6. Click the "Log In" button.
7. You will then have an active Internet connection.

NOTICE: The Limestone-Guest WiFi network is unencrypted. Unless you are accessing a web page with HTTPS in the address or using an application that encrypts the data being transmitted, all of your transmitted and received data will be sent in plain text and could possibly be intercepted by a third party.