



## GEORGIA GWINNETT COLLEGE - NETWORK & INTERNET USAGE PROCEDURE

The Georgia Gwinnett College (GGC) Network Usage and Internet Usage Procedure provides guidelines for utilizing Internet and network connectivity at Georgia Gwinnett College. All individuals who require network access including faculty, staff, students, and guests are advised to read this document. This document respects the value of the diversity of GGC organizations while providing guidance with regards to information technology (IT) and Office of Educational Technology (OET) operations within the GGC campus.

### STUDENTS

1. All students will connect their devices to the GGC network via wireless connection using the network called ““GGC Wireless”.”
  - a. Students will be asked to enter their GGC username and password when logging in.
2. Students should NOT connect to the GGC network via a wired connection. Wired connections are for faculty and staff use only.
3. GGC’s OET staff members will assist with connectivity failures and Internet service disruption.
  - a. GGC cannot be held liable or responsible for hardware failures, non-compliant software nor denials of service.
4. All wireless users connecting to the “GGC Wireless” network are warned against using file-sharing or “peer-to-peer” software such as BitTorrent, eMule, KaZaA, Limewire etc. for the illegal downloading of copyrighted material.
  - a. Wireless Access Points provide shared bandwidth. File-sharing applications decrease the level of available bandwidth per user. Please show consideration for others.
  - b. Use of file-sharing software is monitored on the campus network and further action may be taken if the GGC network or GGC-owned devices are being used for illegal transfer of copyrighted material.
5. Any visitor or guest should not use the wired network with any personal computing device(s). The “GGC Guest Wi-Fi” network is provided for visitor use.

### FACULTY/STAFF

1. All GGC-owned laptop and workstations should use the wired network as the primary method for accessing the Internet and all GGC network resources. Wired connectivity provides greater security and reduces the usage load on the “GGC Wireless” network.
2. When a wired connection is not available, devices can be connected to the GGC network via wireless connection using the network called ““GGC Wireless”.”
  - a. Faculty/Staff will be asked to enter their GGC username and password when logging in.
3. Faculty/Staff should NOT use the wired network with their personal computing devices.
4. Installation of “peer-to-peer” software such as BitTorrent eMule, KaZaA, Limewire etc. for the illegal downloading of copyrighted material is prohibited on GGC-owned devices and equipment.
  - a. Use of file-sharing software is monitored on the campus network and should not be used for illegal transfer of copyrighted material.
5. Any visitor or guest should not use the wired network with any personal computing device(s). The “GGC Guest Wi-Fi” network is provided for visitor use.

### THE "GGC WIRELESS" NETWORK FOR STUDENTS AT RESIDENTIAL LIFE (RESLIFE)

Georgia Gwinnett College recognizes that students who live at GGC's Residential Life facilities require additional network resources.

1. All students will connect their laptop and other personal devices via wireless on the "GGC Wireless" network.
2. All students will connect gaming consoles and other media streaming devices via wireless on the "GGC PPSK" network.
  - a. Devices allowed on the "GGC PPSK" wireless network
    - i. Gaming consoles (Microsoft Xbox, Sony Playstation, Nintendo Switch, etc.).
    - ii. Media streaming devices (Amazon Fire Stick, AppleTV, Roku, Google Chromecast, etc.).
  - b. The "GGC PPSK" wireless network is broadcasted for residents housed within GGC dormitories.
3. To receive a PPSK code for the "GGC PPSK" wireless network, student will need to open a GGC Helpdesk Request Ticket via email ([helpdesk@ggc.edu](mailto:helpdesk@ggc.edu)) or self-service portal ([helpdesk.ggc.edu](http://helpdesk.ggc.edu)).
  - a. The device's wireless MAC address will be included in the GGC Helpdesk Ticket to receive the PPSK code
4. GGC's OET staff members will assist with connectivity failures and Internet service disruption.
  - a. GGC cannot be held liable or responsible for hardware failures, non-compliant software nor denials of service.
5. The "GGC Guest Wi-Fi" network is provided for visitor use.

### HARDWARE & SOFTWARE REQUIREMENTS

Georgia Gwinnett College requires that all devices that connect to the GGC Network have a minimum level of security protection built into the hardware of the device. Also, a device must have adequate and up-to-date software virus protection.

All devices must meet the following criteria:

- A minimum of Microsoft Windows 7 Service Pack 1
- A minimum of Apple El Capitan (10.1.1)
- The latest Microsoft or Apple security updates
- Up to date anti-virus software
- A compatible 802.11 b/g/n wireless adapter
- An 802.1x compliant adapter

### VIRUS & SPYWARE PREVENTION:

A computer virus is a program which invades your computer and contains code that has the potential to cause damage and/or perform unwanted/unauthorized functions. Computer viruses have impacted a significant number of computers worldwide. There are over 10,000 known computer viruses. Over 200 new viruses are being discovered every month.

Spyware is software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet. However, it should be noted that the majority of shareware and freeware applications do not come with spyware. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability.

1. GGC requests that ANTI-VIRUS and/or ANTI-SPYWARE SOFTWARE to be installed and active on all devices connected to the "GGC WIRELESS" Network
  - GGC minimally recommends using Microsoft Security Essentials for any device installed with Microsoft Windows 7 or 8
    - It is a free download from Microsoft:  
<https://support.microsoft.com/en-us/help/14210/security-essentials-download>
  - GGC minimally recommends using Microsoft Defender for any devices installed with Microsoft Windows 10
    - It is a native application installed with Microsoft Windows 10
  - GGC minimally recommends using Malwarebytes for MAC on all Apple devices
    - It can be downloaded for free from Malwarebytes:  
<https://www.malwarebytes.com/mac/>

### UNACCEPTABLE ACTIVITIES

Georgia Gwinnett College will not support or condone the activities listed below:

1. Activities which excessively consume Network Resources
2. Activities which violate the Network Policies
3. Activities which violate Local, State or Federal Law, and/or International Treaty
4. Activities which interferes with the legitimate function of other devices connected to GGC
5. Commercial Activities not approved by GGC
6. Sending Spam (Unsolicited Bulk and/or Commercial Email)
7. Open E-Mail Relays
8. Denial of Service Attacks
9. Hacking
10. Cracking
11. Probing, scanning or other activities that learn about GGC connected devices
12. Packet/Content Sniffing
13. Unauthorized access to VM Guest or Hosts Server(s)
14. Illegal distribution of any copyrighted material
15. "Stealing" or "Borrowing" IP addresses

GGC will work in cooperation with law enforcement agencies when a crime is committed. For incidents which do not warrant involvement of law enforcement agencies, GGC disciplinary action may be required up to and including termination or expulsion. The offending device(s) will be removed immediately from the GGC's infrastructure and network.