

The George Washington University has policies and codes of conduct that govern the use of University computers and networks. In order to facilitate the administration of ResNet service and to maintain equitable use of network resources, additional policies apply to the use of this service.

By registering for ResNet service you agree to abide by the ResNet Code of Conduct. Please read this document carefully. Updates to the Code of Conduct can be found on the STS Web site: <http://iss.gwu.edu/sts>. ResNet users are responsible for adhering to the most current Code of Conduct.

ResNet users who violate any aspect of the Code of Conduct may be subject to judicial action and/or temporary or permanent loss of their ResNet connection. ResNet connections may be temporarily suspended without advance notice if a user is in violation of the Code of Conduct.

No Shared Connections: One network connection is supplied by ResNet for use by registered individual users. ResNet users cannot use any mechanisms (either hardware or software) to provide network connectivity to non-registered users, including the establishment of a server. The use of routers and/or similar networking devices and Internet connection sharing software is prohibited unless advance authorization is granted by ResNet and is limited to personal and academic use by the subscriber. The establishment of private networks is strictly prohibited unless authorized in advance by ResNet. Exceptions to this policy are considered for academic purposes only and require written documentation from the professor or responsible academic professional. ResNet reserves the right to evaluate, then grant or deny requests for exceptions.

IP Address Usage: ResNet subscribers use a single IP address for use in a wired GW residence hall. The use of any IP address other than one assigned by ResNet is prohibited. Subscribers who change residence halls should notify ResNet to ensure accuracy of registration information. Use of unassigned IP addresses can cause conflicts, possibly resulting in a disruption of service for the person assigned that address. Use of unauthorized IP addresses may result in loss of ResNet services and possible judicial action.

General Usage: Computers connected to the University network are governed by policies and codes as well as federal, state, and local laws. Among other restrictions, the operation of any commercial or for-profit enterprise or advertising is prohibited, along with any re-sale of access or services. Illegal activities, including, but not limited to such practices as fraud, harassment, e-mail spamming, software piracy, and copyright infringement are prohibited. In addition, IP spoofing, packet sniffing, virus distribution, or any activity that disrupts the University network or computing resources are violations of the Code of Conduct for Users of Computing Systems and Services at The George Washington University which applies to all ResNet users. Any user/computer suspected of involvement in an illegal activity or of posing a threat to the network because of a virus, hack, excessive bandwidth use or other activity, will be removed from the network

until the matter is resolved. Violation of the Code of Conduct may also result in an individual permanently losing the privilege of a ResNet connection.

Wireless in the Residence Halls: The establishment of wireless networks is not authorized in the residence halls due to security concerns. Unauthorized and unsecured wireless networks allow the theft and monitoring of personal information as well as allows a system to be open to destructive hacking. Establishing a wireless network or using a wireless access point within a residence hall may be subject to judicial action and permanent loss of your ResNet connection.

Network Security: GW currently implements an access control list that prevents computers outside the University to connect to the GW network and computing resources. The access control list is a University-wide security measure to prevent unauthorized access. Certain networking software will not run properly through the access control list. Please contact STS for additional information. No exceptions can be made to the access control list, even to allow gaming devices network connectivity. GW also employs the use of Cisco Clean Access (CCA) on the GW network. CCA enforces University policy by scanning computers to determine whether security requirements have been met by all computers using the network (*see Security and Virus Protection*). Security of individual computers on the GW network is ultimately the responsibility of the user. STS reserves the right to remove a computer from the network if it poses a risk to other computers. Meeting the security requirements enforced by CCA is required and full access to the Internet will be restricted until security requirements have been met. The University reserves the right to place restrictions on the use of its computers, network systems and resources to maintain security of user networks.

User Responsibility: Students are responsible for use of their personal computer, including use by other individuals. Furthermore, users are responsible for use of any computer on which the user has logged in using their NetID. Users will be held accountable for any violations that occur involving their personal computer or for activity conducted while logged in with their NetID. Students should only allow others to use their machine with the full understanding of the consequences of that action. STS discourages the use of Microsoft File Sharing and similar programs. Should the user choose to enable this option, the user must understand that their files will be vulnerable. In addition, it is the responsibility of the computer owner to maintain reasonable security (disabling anonymous access, maintaining accurate logs, using strong passwords, etc.). Computers with inadequate security are often used by hackers to gain access to other campus hosts. Any computer involved in a break-in attempt will be disconnected from the campus network immediately. Users may not tamper with any of the wall jacks in their room. Should a user tamper in any way with a wall jack, that user will be held financially responsible for repairs.

Security and virus protection: Secure computing is a partnership between the user and the University. Each ResNet user is responsible for the security of his or her computer. Users are required to use GW provided Symantec Anti-Virus software on their computer and set the software to automatically Live Update and perform a weekly system scan.

Additionally, Windows users must enable Automatic Updates. Prior to connecting to the GW network, users must make every reasonable attempt to ensure that their computer is secure, updated, and protected.

STS is not responsible for the security of any computer using our network. Individual users are responsible for the security of their computers.

Support: STS is a customer service division of Information, Systems and Services (ISS) dedicated to providing support to GW student users. STS operates a technician-staffed telephone support hotline for troubleshooting as well as for scheduling in-room technician appointments. Troubleshooting must be performed by telephone before an in-room appointment can be scheduled. The ResNet user must be present in order for an STS technician to service a connection. If a user is not present for a scheduled appointment, the appointment will be rescheduled on a first-come, first-served basis. STS technicians will test the networking equipment provided by STS as well as the wall jack. Should the technician determine that the wall jack is broken, the problem will be reported to the appropriate office for repair. Users who are in need of virus/hardware/software support should bring their computer to the ISS Student Technology Services (STS) City Hall location.

Wall Jack Repair: STS technicians are trained to determine if a residence hall network wall jack is functioning properly or is broken and in need of repair. STS does not perform repairs on wall jacks but instead refers these repairs to the group responsible for network jack repair. Routine repairs generally take 3-5 business days. Complicated repairs may take longer. All repairs may take longer than 3-5 business days at the start of the fall semester when repair request volume is higher than normal. Repair times are variable depending on the problem and the responsible department. STS is not responsible for the length of time necessary to repair a network wall jack.

Any special networking requests that exceed the bounds of the ResNet Code of Conduct are subject to approval by ISS Management and require prior academic approval. Please contact STS for details. STS staff will make a "best effort" to provide hardware and software support for students.