

Dorm Internet Access Agreement

St. Mary's Preparatory has provided for its' resident students access to a high- speed connection to the World Wide Web.

Equipment needed for connection to the dorm network includes a Network Interface Card (NIC), and a Category 5 patch cable. Users are urged to purchase and maintain anti-virus software, such as Norton Anti-Virus, McAfee, Sophos and others. Installing anti-virus software and keeping your virus definitions up to date will protect your PC from damage and loss of valuable data. It is also important that you keep your software up to date through the use of Windows Update. See www.microsoft.com/security for more detailed information on how to keep your computer secure from viruses and threats.

St. Mary's Preparatory is responsible for securing its network and computing systems in a reasonable and economically feasible way against unauthorized access and/or abuse while making them accessible for authorized and legitimate users. This responsibility includes informing users of expected standards of conduct and the disciplinary measures for not adhering to them. Any attempt to violate the provisions of this policy will result in disciplinary action. Such action may be in the form of temporary or permanent revocation of user access, regardless of the success or failure of the attempt. In addition, School Administration may take disciplinary action.

The users of the network are responsible for respecting and adhering to local, state, federal, and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities. If such an event should occur, this organization will fully comply with the authorities to provide any information necessary for the litigation process. While we cannot be responsible for the actions of individual users, it is understood that St. Mary's Preparatory will make every effort to ensure compliance with established laws. The Students are also bound by The St. Mary's Honor Code during these off hours and computing times.

We will monitor all network activity, incoming or outgoing, on the dorm network and on all computers internally tied to it. All Web usage is logged by default. The high-speed access to the World Wide Web is behind a Firewall server & Web Filtering Device, and has been filtered to only allow connection through TCP/IP port 80, which is the standard port for Web page access. All other TCP/IP ports have been blocked for your safety and protection. Viruses and hackers can and do use other TCP/IP ports to gain access to your computer, or to spread viruses. Another reason is to block the use of Peer-to-Peer file sharing networks (KaZaA, Gnutella Morpheus, LimeWire, Gnucleus, Bearshare, Aimster, iMesh) that are used to share copyrighted material in violation of the Federal Digital Millennium Copyright Act. Since the sharing of such copyrighted material is illegal, students are blocked and prohibited from using file sharing networks. You should also be aware that law enforcement agencies, the Recording Industry Association of America (RIAA), and other copyright holders of digital media are actively monitoring the Internet for users who are distributing copyrighted material. The recording, film and software industries have recently become very aggressive in their active pursuit of copyright infringement. They have spent millions of dollars, and they have hired hi-tech firms to develop and maintain

software that is able to search the Internet and identify unauthorized distribution of their protected titles. This active monitoring is specifically designed to search for distribution of materials using the above listed software packages. Attempting to set up any other kind of server on the dorm network is prohibited, and automatically blocked by the Firewall server.

The willful introduction of computer viruses or other disruptive/destructive programs into the dorm network or into external networks is prohibited. Use of systems and/or networks in attempts to gain unauthorized access to remote systems is prohibited. Decryption and/or capture of system or user passwords is prohibited. The copying of system files is prohibited. The copying of copyrighted materials, such as third-party software, without the express written permission of the owner or the proper license is prohibited. The intentional attempt to crash network systems or programs is a punishable disciplinary offense. Any attempt to secure a higher level of privilege on network systems is a punishable disciplinary offense.

Network users are responsible for all traffic originating from their network device. In addition, network traffic is considered private, thus, any attempts to read or monitor network information of others ("sniffing") is a violation of the privacy act. Repeat violations will result in the school disconnecting the device from the network. Attempts by individuals to reconfigure the network infrastructure can result in damage to the infrastructure or severe network problems. Examples of this are extending the network with hubs/switches/repeaters/wired and/or wireless routers, daisy chaining of wiring and the use of non-standard electronics and wiring. Where damage is found to be caused by an individual, repair costs will be billed accordingly. When a user is encountering problems related to non-adherence to industry and/or St. Mary's network standards by installing their own wiring and/or electronics, the user risks being removed from the network. Please keep in mind that you are responsible for all uses of your computer, and that network use by a computer can be traced to its' owner. Remember, dorm network access is a privilege, not a right. Please use the privilege in a responsible manner, and you will be able to surf the Web with ease.

Dorm Room Internet Access Agreement

I, _____ (resident), having received and read the St. Mary's Preparatory dorm room Internet access agreement to follow all codes, policies, procedures and rules mentioned in the agreement, not excluding upholding the schools honor code as well. I acknowledge and agree to all of the terms and conditions and agree to uphold all Catholic/Christian morals, values and principles to all Internet usage. Any violations of these values on the Internet will result in the immediate loss of the computer and/or internet connection. Finally, I understand that the Dean of Resident Students and IT Director may deactivate and limit the internet access at their own discretion.

Resident Signature

Date

Dean of Resident Students Signature

Date