



COMPUTER AND SYSTEMS USAGE POLICY

All persons using the School's computers, the School's computer systems, or personal computers on School property or over the School's systems are required to abide by the following rules. This policy also applies to the use of any personal electronic devices (computers, cameras, phones, video cameras, PDA, etc.) on school property or at a school related event. Failure to abide by these rules will result in appropriate disciplinary action determined by the School administration. All computers should be used in a responsible, ethical and legal manner. Violations of the following guidelines may result in the revocation of access privileges and possible disciplinary responses, including expulsion for serious offenses.

Purpose: The purpose of providing access to the Internet and the School's computer systems is to support research and provide unique educational opportunities. The use of such resources should be limited to those activities that support the School's educational objectives.

Privilege: The use of the School's systems is a privilege and not a right. Inappropriate or illegal use of the School's systems or of the Internet will result in loss of the privilege and disciplinary action.

Internet Access: The School community--students, faculty, administrators and staff--have the privilege of full access to the Internet. The School encourages students and teachers to use the Internet to expand their knowledge. The Internet allows users to send and receive e-mail, to log onto remote computers, and to browse databases of information. It also lets users send and receive files and programs contained on other computers. Files may be downloaded only to personal disks. Files are not to be downloaded to the Schools local or network hard drives.

The School does not provide any type of filtering system. Although doing so generally can eliminate access to offensive and pornographic materials, it also has the negative effect of filtering out genuine educational materials. In addition, no filtering system is foolproof. Therefore, we expect users to act responsibly in their searches and to immediately disengage from any materials that are inappropriate and to report the situation to the faculty member or administrator in charge of the activity. Although the School cannot effectively restrict the content of information obtained by students via the Internet, obtaining material that is explicitly labeled, as not intended for minors will be considered a violation of School rules. Furthermore, making public or passing on any material that is pornographic, violent in nature, or otherwise harassing is totally unacceptable and will be dealt with immediately by the appropriate administrator.

Internet Safety: Students should never give out personal information (address, telephone number, name of School, address of School, date of birth, Social Security Number, credit card number, etc.) over the Internet. Students also should not meet with someone that they have contacted on-line without prior parental approval. Safety is the responsibility of the parent and student. The School is not liable in any way for irresponsible acts on the part of the student.

Pirated Software: The term "pirated software" refers to the use and transfer of stolen software. Commercial software is copyrighted, and each purchaser must abide by the licensing agreement published with the software. There is no justification for the use of illegally obtained software. The School will not, in any way, be held responsible for a student's own software brought to School for personal use.

Network Access: Accessing the accounts and files of others is prohibited. Attempting to impair the network, to bypass restrictions set by the network administrator, or to create links to the School's web page is prohibited. Obtaining another's password or rights to another's directory or e-mail on the network is a violation of School rules as well as a form of theft. Taking advantage of a student who inadvertently leaves a computer without logging out is not appropriate. Using someone else's password or posting a message using another's log-in name is a form of dishonesty, just as is plagiarism or lying, and will be treated as a violation.

School's Right To Inspect: The School reserves the right to inspect user directories for inappropriate files, emails, and pictures and to remove them if found and to take other appropriate action if deemed necessary, including notification of parents. The School also reserves the right to inspect any personal electronic devices brought onto campus. Do not assume that any messages or materials on your computer or the School's systems are private.

E-mail: RASG community members and High School students have an Email account that is protected by username and password. Members should not reveal their username or password, or other personal information in an email or to any other member of the RASG community. Electronic mail cannot be used to harass or threaten others. Members are to refrain from the use of obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language in emails or accessing or maintaining a presence on an Internet site demonstrating the same content.

The School reserves the right to randomly check e-mail or text messages. Students should be made aware that deleted e-mails can be undeleted. Members are not allowed to send messages that will disrupt network resources (i.e. chain mail, virus hoaxes, spam, etc.). Any email violation will be considered a direct violation of this policy and will be dealt with accordingly.

Chat Rooms, Instant Messaging, and Social Networking Sites: Participation in “chat rooms,” instant messaging, posting messages, blogs, or browsing social networking sites (such as MySpace, EZBoard, YouTube, or any others similar sites) on campus or using School equipment is prohibited. In addition, any person who believes that they have been harassed or threatened by any of these methods of communications should immediately report the concern in accordance with the School’s No Harassment/No Bullying policy. Students should also be aware that teachers and administrators periodically check such sites and may determine that off campus behavior violates the School conduct code by making disparaging or negative comments about the School, administration, or faculty members in a manner that is disruptive to the School’s educational mission or activities.

Viruses: Every effort is made by the School to keep our system virus-free. Even with the best techniques, however, computer viruses can be transmitted to and from any computer, including those in the computer center. The School is not responsible for the transmission of any virus or for damage suffered from a virus.

Computer Care: Members of the School community will not abuse, tamper with, or willfully damage any computer equipment, use the computer for other than appropriate work, or bring food or drink into any computer area. Any intentional acts of vandalism will result in discipline and students will be held responsible for replacement or repairs.

Reporting Requirements/Discipline: Any student, who accesses inappropriate material on the Internet, receives harassing, threatening, or inappropriate materials via e-mail or on the Internet, must immediately report the concern to the teacher who is supervising the activity or to an administrator so that the situation can be investigated and addressed appropriately. Students who violate any aspect of this Computer and Systems Usage Policy will be subject to appropriate discipline and loss of computer or Internet privileges.

Prohibited Uses:

- School classroom technology resources may not be used for personal, commercial or financial gain. All data and software must be of an educational nature. RASG community members are provided a username and password to access the RASG computer network.
- Members may not reveal their username or password to any other member. Any suspect activity with a student account should be immediately reported. Damage that results from a security breach related to the misappropriation of a member’s network identity will result in both parties being prosecuted under the RASG handbook and where appropriate Florida law.
- Community members are not allowed to download any executable files to RASG computers unless directly related to an educational activity. This includes games, videos, zip files, wave files, programs, screen savers, and desktop backgrounds, etc. Any downloads will be considered a direct violation of this policy and will be dealt with accordingly.
- Community members must not access or attempt to access any of the school’s restricted LAN sites and/or programs. Doing so will be considered among the most major offenses and will be dealt with accordingly.

RASG RETAINS THE RIGHT TO POST ON OUR WEBSITE, PICTURES AND GENERAL TEXT, SUCH AS THAT FOUND IN NEWSPAPERS, IN REGARDS TO STUDENT ACTIVITIES FOR GRADES K-12.