Computers

St. Mary's Charter School ("School") electronic communications systems, including its network and access to the Internet, are primarily for administrative and instructional purposes. Limited personal use of the system is permitted if the use:

1) Does not result in any direct cost paid with State funds, or if the School's Charter Holder is reimbursed for any direct costs involved;
2) Does not relate to private commercial purposes; and
3) Involves only incidental amounts of employee time, comparable to reasonable coffee breaks during the day.

Some employees are given access to the Internet to assist them in the performance of their jobs. Employees may only access the Internet through the School's approved Internet firewall.

All School computer resources are School property, and any information located in or on computers and e-mail/voice mail systems is also School property and will be subject to inspection by the School.

E-mail and Voice Mail Systems

All messages sent, received, composed and/or stored on these systems are the property of the School. E-mail transmissions and other use of the School's electronic communications systems are not confidential and can be monitored at any time to ensure appropriate use.

Confidentiality

Employees shall not use a password, access a file, or retrieve any stored information unless authorized to do so. Employees may not attempt to gain access to another employee's files/messages.

Privacy

All files and messages on School computers are School property. They are not the property of any employee, even if created by an employee. Anything created on the computer or Internet may, and likely will, be reviewed by others. If necessary, employees shall take steps to help protect the security of documents. The School has the right, but not the duty, to monitor any and all aspects of its computer system, including, but not limited to, monitoring sites employees visit on the Internet. Employees have no expectation of privacy in anything they create, store, send, or receive on their workplace computer, the School network, or Internet resources.

Restrictions

1) Employees are not allowed to use School computer resource for any reason other than official School business, except limited use describe above.
2) Employees may not use e-mail or the Internet to send or receive materials, proprietary financial information, or other similar materials that violate copyright law.
3) The e-mail system may not be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages that contain sexual implications, racial or gender-specific slurs, or any other comment that offensively addresses an individual's age, sexual orientation, religious or political beliefs, national origin, disability, or anything that could be construed as harassment or disparaging of others.
4) Employees should refrain from sending non-business related e-mails to other School employees or persons outside the School system, except as described above.
5) The School is responsible for maintaining records of software licensing agreements for the School. In order to ensure compliance with copyright laws and software licensing agreements, and help prevent computer viruses from being transmitted through the system, employees are not permitted to install or download any software or content, such as music, videos, or non-work related "zipped" files onto the School's computer system without prior approval from the Campus Principal or designee.
6) Unauthorized duplication of software, often referred to as "piracy," is a federal crime. Employees are not permitted to make, acquire, or use unauthorized copies of computer software.

Employees who are authorized to use the School's electronic communications systems are required to abide by the provisions of this policy and any related administrative procedures. Failure to do so can result in suspension or termination of privileges and may lead to disciplinary action, up to and including termination of employment. Employees should notify their immediate supervisor(s) or the Information Systems Department upon learning of violations of this policy.