

COMPUTER, EMAIL AND INTERNET POLICY

Computers, computer files, the e-mail system, and software furnished to employees are School property intended for School use only. Employees should not use a password, access a file, or retrieve any stored communication without authorization. To ensure compliance with this policy, computer and e-mail usage may be monitored and/or checked periodically.

The School strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, the School prohibits the use of computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassment or showing disrespect for others.

E-mail may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-school matters.

The School purchases and licenses the use of various computer software for School purposes and does not own the copyright to this software or its related documentation. Unless authorized by the software developer, the School does not have the right to reproduce such software for use on more than one computer.

Employees may only use software on local area networks or on multiple machines according to the software license agreement. The School prohibits the illegal duplication of software and its related documentation.

Employees should notify their immediate supervisor, the School Administrator and or the Principal or any member of management upon learning of violations of this policy.

Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

Internet Usage

Internet access to global electronic information resources on the World Wide Web is provided by the School to assist employees in obtaining work-related data and technology. The following guidelines have been established to help ensure responsible and productive Internet usage. The Internet usage is intended for job-related activities to do with the School only and not for personal use.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the School's business operations and, as such, is subject to monitoring and/or periodic checking by the School management. Consequently, employees should always ensure that the school information contained in Internet e-mail messages and other transmissions is accurate, appropriate, ethical, respectful and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of School. Therefore, the School reserves the right to retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.

Data that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person. Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not got

authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights.

To ensure a virus-free environment, no files may be downloaded from the Internet without prior authorization

Abuse of the Internet access provided by the School in violation of law or School policies will result in disciplinary action, up to and including termination of employment.

Employees may also be held personally liable for any violations of this policy. The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and resources for personal gain
- Stealing, using, or disclosing someone else's code or password without authorization
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization
- Violating copyright law
- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions
- Sending or posting messages or material that could damage the organization's image or reputation
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
- Using the Internet for political causes or activities, religious activities, or any sort of gambling
- Jeopardizing the security of the organization's electronic communications systems

- Sending or posting messages that disparage another organization's products or services
- Passing off personal views as representing those of the organization
- Sending anonymous e-mail messages
- Engaging in any other illegal activities

Use of Social Media

The use of social networks such as web based discussion or conversation pages and other forms of social networking such as Facebook, Twitter, etc. as significant new forms of public communication is strictly prohibited. As such, we hold all of our employees who engage in social networking to the same standards we hold for any public communications such as: comments to a TV, radio or news reporter. Therefore, all employees have an obligation to this School to ensure that no public communication is made, including social networking communications. Any employees found to socially network using the above type of media and create a negative impact to the reputation of the school or bring disrepute in any way to the School, its employees, parents, children, suppliers, etc; will result in disciplinary action.

Further, only a select group of employees may be authorized to publicly speak on behalf of the School. Therefore, employees must have prior authorization to be a School spokesperson to the extent their social networking communications represent, or appear to represent the official School view or perspective on any particular topic. Violations of this policy will result in discipline which may include termination, depending on the severity of the situation and its impact on the School.

Identified below are general guidelines and examples of prohibited communications. Please note that this list shows examples only and is not intended to be, nor is it, an exhaustive list of prohibited communications. Instead, we have included this list to provide you guidance with respect to your social networking and other public communications.

General Guidelines and Examples of Prohibited Communications select group of employees may be authorized to publicly speak on behalf of the School

- Assume at all times you are representing our School when engaging in any form of social networking.
- Exercise discretion, thoughtfulness and respect for your colleagues, business associates, customers, and our partners.
- Do not discuss internal policies or operations issues in any manner that could reflect poorly on the School.
- Do not engage in public criticism or disparagement of School personnel, customers, partners, suppliers or competitors.
- Confidential or proprietary company information or similar information of third parties who have shared such information with our School should not be shared on any social networking site.
- Be mindful that all public communications that reference our School, including social networking communications, are subject to review by our School, and may lead to discipline to the extent the public communication harms our School.