

Integrated Day Charter School

Governing Board



Policy Series: 4000

Policy Number: 4118.4/4218.4
4118.5/4218.5

Personnel

Internet and E-mail Usage

The School considers the Internet a valuable resource. As such, it should be thought of as another source of information and communication, and given the same consideration as paper resources. Like the Wall Street Journal, the Journal of Accountancy, and other publications, the Internet is a valuable resource with a variety of uses. However, the School expects staff members to exercise professional judgment when accessing the Internet. Common sense and judgment will help ensure the Internet remains a vital tool and resource instead of a security threat. While the School encourages Internet usage to improve business productivity, any abuse may result in disciplinary action up to and including termination. The following outlines the appropriate use of the Internet by School employees.

a. Internet access is provided to employees solely for business purposes. Business purposes include communication with educational resources; communication with other employees; research; information retrieval; and other business tasks designed to achieve the School's business objectives. Correspondence and communications over the Internet should be in good taste, avoiding offensive, discriminatory, or harassing language. Also, a diligent effort should be made to avoid spelling and grammatical mistakes.

b. Some examples of inappropriate Internet usage are listed below. This should not be considered an exhaustive or all-inclusive list.

- To access obscene, sexually explicit, or politically subversive material.
- To communicate discriminatory, harassing, or obscene correspondence or material.
- To use it for personal gain, non-School solicitation, or illegal activity.
- To distribute unlicensed software.
- To represent yourself as someone else.
- To access servers for which you have no authorization.
- To use resources to alter, damage, or destroy information.
- To use it for any purposes that are contrary to the best interests of the School.

- c. The School recognizes that some personal use of the Internet is unavoidable. Nevertheless, personal use should be kept to a minimum and should be in accordance with the standards of good taste described in this policy. Personal Internet use is comparable to existing telephone/fax usage policy, and if possible, should be deferred to non-business hours.
- d. To prevent computer viruses from being transmitted through the School's E-mail/Internet system, employees will utilize the school's anti-virus software to check for viruses and clean, if necessary, all files brought in from outside the school.
- e. The School will monitor, audit, and otherwise control access to the Internet from its networks as well as through Internet Service Provider accounts.
- f. Confidential, proprietary, and sensitive information should not be communicated through the Internet. You should assume that unauthorized people might intercept all communications.
- g. Any School documents transferred via the Internet must clearly indicate our School as the holder of the copyright. Employees must respect the copyrights of all materials obtained over the Internet.
- h. All electronic documents created or stored, and all communications using the School's computers, are the property of the School. The School may access documents or communications stored on its property or in its systems whenever warranted by business need or legal requirements, and it will monitor its systems to ensure proper use and to prevent security violations. Employees should not expect that their communications using the School's systems are private or confidential.
- i. Any violation of this policy will be subject to restriction or loss of access and other corrective action up to and including termination. The School also has the right to notify the appropriate authorities if it discovers evidence of any possible illegal activities.
- j. Any employee who has witnessed misuse of the Internet including nonconformance to this policy, potential exposure to viruses, and unauthorized access should immediately report violations to the Director.