

## *Addendum B*

### **7.33 USE OF ELECTRONIC RESOURCES**

The Pinellas County school district (“the district”) provides electronic resources (including, but not limited to, computers, networks, software, Internet access, and facsimile machines) to support the educational mission of the schools, to enhance the curriculum and learning opportunities for students and school staff and to conduct district business.

**1. Property of the District; No Expectation of Privacy:** The district retains control, custody and supervision of all electronic resources owned or leased by it. All messages

created, sent, or retrieved through electronic resources are the property of the district. Any information generated, stored or sent through electronic resources is the same as any written document and may be subject to Florida’s public records act, Chapter 119, Florida Statutes. The district reserves the right to monitor all use of electronic resources by employees and other users. Employees have no expectation of privacy in their use of electronic resources.

**2. Acceptable Uses:** Employees are to use the district’s electronic resources for school related purposes and performance of job duties consistent with the district’s strategic directions and goals. Users may access the network only through district-owned computers and access points. When using electronic resources, all users must adhere to the provisions of this policy, the district’s standards of conduct, and the Code of Ethics and Principles of Professional Conduct of the Education Profession in the State of Florida, Rules 6B-1.001 and 6B-1.006, F.A.C.

**3. Incidental Personal Use:** Incidental personal use of electronic resources is permitted as long as such use does not interfere with the employee’s job duties and performance, with system operations or other system users. “Incidental personal use” means use by an individual employee for occasional personal communications, in the same manner as an employee might reasonably use the district’s telephone for occasional personal calls. Such personal use must comply with this policy.

**4. Unacceptable Uses:** General rules and expectations for professional behavior and Communication applies to use of the district’s electronic resources. Examples of unacceptable uses that are prohibited include, but are not limited to, the following:

a. Any use that is illegal or in violation of other district policies, including harassing, discriminatory or threatening communications and behavior. Harassing, defamatory, insulting, or profane language or pictures are not permitted. It is not permitted to transmit messages with derogatory or inflammatory remarks about a person’s race, color, sex, creed, religion, legal marital status, national origin, age, handicap, physical attributes or sexual orientation.

b. Any use involving materials, language or pictures that are obscene, pornographic,

sexually explicit or sexually suggestive.

c. Any inappropriate communications with students or minors.

d. Any use for private commercial, advertising or business solicitation purposes.

e. Any use of electronic resources as a forum to solicit, advocate or communicate the

personal, political or religious views of an individual or non-school-sponsored organization.

However, the district may establish limited forums to solicit and communicate the personal views of employees or members of the public on specific topics. The Superintendent or designee shall determine the appropriate hour and duration that a forum will be available.

f. Any use to raise funds for any non-school-sponsored purpose, whether profit or

not-for-profit, except as approved by the superintendent or designee.

g. Any use to convey a threat of violence.

h. Any use to disseminate false information that impacts the credibility of the district.

i. Any communication that represents personal, political or religious views as those of the district or that reasonably could be misinterpreted as such.

j. Opening or forwarding any e-mail attachments (executable files) from unknown sources or that may contain viruses. Employees should take all necessary precaution to

prevent viruses from entering the district's network.

k. Sending or forwarding mass e-mails or chain letters to district users or outside parties for district or non-district purposes without the permission of the principal or department administrator ("site administrator").

l. Any use that disrupts a district activity, including but not limited to the district's electronic resources. Deliberate attempts to degrade or disrupt systems performance will be viewed as criminal activities under applicable state and federal law.

m. Any misuse or damage to the district's electronic resources.

n. Misuse of computer passwords or accounts. Users may not use others' passwords

without their explicit permission and may not share passwords with others.

Employees should change their passwords at least quarterly to protect the security of the network. Trespassing in others' folders, documents, or files is unacceptable. The employee is responsible for his/her actions and activities involving district electronic resources, and for his/her computer files, passwords and accounts.

o. Any attempt to access unauthorized sites by bypassing the district's Internet filtering system

This policy provides general guidance and examples of prohibited uses for illustrative

purposes, but does not attempt to state all required or prohibited activities by users.

Employees or other users who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the site administrator. If the site administrator is unsure of the answer, the site administrator should contact the office of Instructional Technology or MIS

**5. Supervision By Staff:** Employees who have the responsibility to supervise students or staff shall provide that supervision during the use of electronic resources.

**6. Confidential Information:** Users may not share confidential information on students or employees with users who are not authorized to have such information. All users who have access to or may have access to personally identifiable student records shall adhere to all standards included in the Family Education Rights and Privacy Act (FERPA); Protection of Pupil Rights Amendment Act (PPRA); section 228.093 and 231.291, Florida Statutes; and other applicable laws and regulations, as they relate to the release of student and employee information.

**7. Copyright Infringement:** Policy 8.15, *Reproduction of Copyrighted Material*, will govern the use of material accessed through the district network. It is a violation of the copyright laws to load software onto a district computer without a license authorizing the use of that software on that computer. Employees shall take reasonable precautions to prevent the copying or the use of unauthorized copies of software on district equipment, and to avoid the use of single copies of software or CD-ROM products across a network with multiple users unless such use is permitted by the application license agreement.

**8. Unauthorized charges:** The district assumes no responsibility for any unauthorized charges made by employees, including, but not limited to, credit card charges, subscriptions, long distance telephone charges, equipment and line costs, or for any illegal use of its computers such as copyright violations.

**9. No Warrantee:** The district makes no warranties of any kind, either expressed or Implied, for the service it is providing. The district will not be responsible for any damages suffered. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or errors or omissions including any and all viruses. Use of any information obtained via the Internet is at the user's own risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through its services.

**10. Penalties for Non-Compliance:** Failure to comply with this policy may result in suspension or revocation of the user's privilege of access, and may subject the user to civil liability or criminal charges. Employees may also be subject to disciplinary action up to and including termination as defined in Policy 8.25

#### DISCIPLINARY GUIDELINES FOR EMPLOYEES.

Statutory Authority: 230.03(2), 230.22, 230.23, 230.23005 F.S.

Laws Implemented: 231.41, 231.381, 231.39, 231.40, 231.481, F.S.

History: New: 7/30/02 Amended 4/13/04