JCS-Inc.
Administrative
Regulations

4010.2 Email and Internet: Communication Systems Administrative Regulations

Effective Date: September 8, 2017 Approved by: Board of Directors

Procedure:

1. JCS, Inc. (JCS) reserves the right to review, audit, intercept, access, and disclose all messages created or received within the file storage and messaging systems to ensure the systems are not being misused. This includes Internet usage and any messages received via the voice mail system.

2. Where required for school business purposes, it may be necessary to inspect the file storage system, message system, and review, copy, or delete any files or messages and disclose the information in both systems to others.

3. JCS reserves the right to review all computer databases and transmissions.

4. All employees should take precautions so as not to transmit a virus through the networks.

5. Employees must not share passwords. Employees shall not use a code, access a file, or retrieve any stored information unless authorized to do so and should not attempt to gain access to another person's files or passwords without the latter's permission.

6. JCS does not condone the illegal duplication of software. The law protects the exclusive rights of the copyright holder and does not give users the right to copy software unless the manufacturer does not provide a backup copy. Unauthorized duplication of software is a Federal crime. Penalties include fines of as much as $250,000 and jail terms of up to five years.

7. JCS licenses the use of computer software from a variety of outside companies. It does not own this software or its related documentation and, unless authorized by the software manufacturer, does not have the right to reproduce it.

8. If an employee learns of any misuse of software or related documentation within the company, they must notify the Principals or supervisor immediately.

9. According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages and criminal penalties, including fines and imprisonment. Employees who make, acquire, or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include dismissal.

10. Inappropriate use of the Internet and/or email systems may result in access being revoked, through disciplinary action for misappropriation of school property. Inappropriate use is any activity that may be considered offensive such as; sexually explicit messages, images or cartoons; racial slurs; gender-specific comments or any other comments that may be construed as harassment or disparagement, or others based

on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs; or any remarks that are harmful to morale.

11. Unauthorized use of communication services and equipment for purposes other than " "official" school business is prohibited. They may not be used for personal business, to send unsolicited information or other non-job related purposes.

12. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. Additionally, all messages composed, sent, or received on the e-mail system are now and remain the property of the school. They are not the private property of any student or employee.

13. Employees may use hardware/software and electronic/voice mail systems provided by the company for school business only.

Original Policy 02/27/01
Revised Policy 09/08/17