EMPLOYEE COMPUTER AND INTERNET USE RULES

The intent of these Board-level rules is to provide employees with general requirements for utilizing the school unit's computers, networks, and Internet services. Administration may implement more specific procedures and rules governing day-to-day management and operation of the computer system to carry out these rules.

These rules provide general guidelines and examples of prohibited uses for illustrative purposes, but do not attempt to state all required or prohibited activities by users. Employees who have questions regarding whether a particular activity or use is acceptable should seek further guidance from the technology director and/or systems administrator.

Failure to comply with Board policy 4.21, these rules, and/or other established procedures or rules governing computer use may result in disciplinary action, up to and including discharge. Illegal uses of the school unit's computers will also result in referral to law enforcement authorities.

A. Access to School Computer, Networks, and Internet Services

The level of access that employees have to the school unit's computers, networks, and Internet services is based upon specific employee job requirements and needs.

B. Acceptable Use

Employee access to the school unit's computers, networks, and Internet services are provided for purposes of administration, education, communication, and research consistent with the school unit's educational mission, curriculum, and instructional goals. General rules and expectations for professional behavior and communication apply to use of the school unit's computers, networks, and Internet services.

C. Prohibited Use

The employee is responsible for his/her own actions and activities involving the school unit's computers, networks, and Internet services, and for his/her computer files, passwords, and accounts. General examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

1. Any use that is illegal or in violation of other Board policies, including harassing, discriminatory, or threatening communications and behavior, violations of copyright laws, etc.
2. Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive.
3. Any inappropriate communications with students or minors.
4. Any use for private financial gain, commercial, advertising, or solicitation purposes.
5. Any use as a forum for communication by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school-sponsored organization, or to try to raise funds for any non-school sponsored purpose, whether for-profit or not-for-profit. No employee shall knowingly provide school e-mail addresses to outside parties whose intent is to communicate with school employees, students, and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or other appropriate administrator.

6. Any communication that represents personal views as those of the school unit, or that could be interpreted as such.
7. Downloading or loading software or applications without permission from the system administrator.
8. Opening or forwarding any e-mail attachments (executable files) from unknown sources that may contain viruses.
9. Sending mass emails to school users or outside parties for school or non-school purposes without the permission of the system administrator.
10. Any malicious use or disruption of the school unit's computers, networks, and Internet services or breach of security features.
11. Any misuse or damage to the school unit's computer equipment.
12. Any misuse of the computer passwords or accounts (employee or other users).
13. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct.
14. Any attempt to access unauthorized sites.
15. Failing to report a known breach of computer security to the system administrator.
16. Using school computers, networks, and Internet services after such access has been denied or revoked.
17. Any attempt to delete, erase, or otherwise destroy, any information stored on a school computer that violates these rules.

D. No Expectation of Privacy

The school unit retains control, custody, and supervision of all computers, networks, and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectations of privacy in their use of school computers, including e-mail and stored files.

E. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

F. Staff Responsibilities to Students

Teachers and staff members who utilize school computers for instructional purposes with students have a duty to supervise such use. Teachers and staff members are expected to be familiar with the school unit's policies and rules concerning student computer and Internet use, and to enforce them. When, in the course of their duties, employees become aware of student violations, they are expected to stop the activity and inform the building principal, technology director, system administrator, or other appropriate person.

G. Compensation for Losses, Costs, and/or Damages

The employee shall be responsible for any losses, costs, or damages incurred by the school unit related to violations of Policy GCSA and/or these rules.

H. School Unit Assumes No Responsibility for Unauthorized Charges, Costs, or Illegal Use

The School unit 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.

I. Connection of Personal Computers to RSU 13 Network

Any computer owned by an employee must be approved by RSU 13 technology staff before being connected to the network or before a student is permitted to use the employee's computer.

J. Employee Acknowledgement Required

Each employee authorized to access the school unit's computers, networks, and Internet services is required to sign an acknowledgement form stating that he/she has read Policy 4.21 and these rules. The acknowledgement form will be retained in the employee's personnel file.

Cross Reference:
Policy GCSA - Employee Computer and Internet Use
Policy IJNDC - Student Computer and Internet Use
Student Computer and Internet Use Rules

Approved: 9/3/09