

EMPLOYEE COMPUTER AND INTERNET USE RULES

These rules accompany Board policy GCSA (Employee Computer and Internet Use). Each employee is responsible for his/her actions and activities involving school unit computers, networks and Internet services, and for his/her computer files, passwords and accounts. These rules provide general guidance concerning the use of the school unit's computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by employees. Employees who have questions about whether a particular activity or use is prohibited are encouraged to contact a building administrator or the Technology Coordinator.

A. Consequences for Violation of Computer Use Policy and Rules

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

B. Access to School Computers, Networks and Internet Services

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

C. Acceptable Use

Employee access to the school unit's computers, networks and Internet services is provided for administrative, educational, communication and research purposes 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.

D. Personal Use

Employees are to utilize the school unit's computers, networks and Internet services for school-related purposes and performance of job duties. Incidental personal use of school computers 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" is defined as use by an individual employee for occasional personal communications. Employees are reminded that such personal use must comply with this policy and all other applicable policies, procedures and rules.

E. Prohibited Uses

Examples of unacceptable uses which 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.. The school unit assumes no responsibility for illegal activities of employees while using school computers.
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, or commercial, advertising or solicitation purposes.
5. Any use as a forum for communicating 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; to solicit membership in or support of 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 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.
6. Any communication that represents personal views as those of the school unit or that could be misinterpreted as such.
7. Downloading or loading software or applications without permissions from the system administrator. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by employees.
8. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the building principal;
9. Any malicious use or disruption of the school unit's computers, networks and Internet services or breach of security features; or misuse of computer passwords or accounts (the employee's or those of other users).
10. Any misuse or damage to the school unit's computer equipment, including opening or forwarding e-mail attachments (executable files) from unknown sources and/or that may contain viruses.

11. Any attempt to access unauthorized sites, or any attempt to disable or circumvent the school unit's filtering/blocking technology.
12. Failing to report a breach of computer security to the system administrator.
13. Using school computers, networks and Internet services after such access has been denied or revoked, and;
14. Any attempt to delete, erase or otherwise conceal any information stored on a school computer that violates these rules or other Board policies or school rules, or refusing to return computer equipment issued to the employee upon request.

F. 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 employees and system users. Employees have no expectation of privacy in their use of school computers, including e-mail messages and stored files.

G. 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.

H. Employee/Volunteer Responsibility to Supervise Student Computer Use

Employees and volunteers who utilize school computers for instructional purposes with students have a duty of care to supervise such use. Teachers, staff members and volunteers 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/volunteers become aware of student violations they are expected to stop the activity and inform the building principal.

I. Compensation for Losses Costs and/or Damages

The employee is responsible for compensating the school unit for any losses, costs or damages incurred by the school unit related to violations of policy GCSA and/or these rules while the employee is using school unit computers, including the cost of investigating such violations. The school unit assumes no

responsibility for any unauthorized charges or costs incurred by an employee while using school unit computers.

Cross Reference: GCSA - Employee Computer and Internet Use

Adopted: 10/16/00

Revised: 12/19/05