EMPLOYEE COMPUTER AND INTERNET USE RULES

Each employee is responsible for his/her actions and activities involving school unit computers, network, Internet services and other technology, 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 allowed or 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 director of information technology.

A. Access to School Computers and Acceptable Use

The level of employee access to school unit computers, network and Internet services is based upon specific job requirements and needs. Unauthorized access to secure areas of the school unit's computers and network is strictly prohibited.

All Board policies, school rules and expectations for professional conduct and communications with others including other staff, students and parents apply when employees are using the school unit's computers, network and Internet services, whether in use at school or off school premises.

B. 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 which violates Policy GCSA and/or other Board policies/procedures or school rules, including harassing, discriminatory or threatening communications and behavior; violations of copyright laws or software licenses; etc. The school unit assumes no responsibility for illegal activities of employees while using school computers computing devices or our network infrastructure.

2. Any attempt to access unauthorized web sites or any attempt to disable or circumvent the school unit's filtering/blocking technology.

3. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive, harmful to minors, or intended to appeal to prurient interests.

4. Any communications with students or minors for non-school-related and/or non-educational purposes.

5. Any use for private financial, commercial, advertising or solicitation purposes.

6. Any use as a forum for communicating 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 any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or not-for-profit. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building administrator or the director of information technology.

7. Any communication that represents an employee's personal views as those of the school unit or that could be misinterpreted as such.

8. Sending mass e-mails (SPAM) to school users or outside parties for any purpose without the permission of the building administrator or director of information technology.

9. Any malicious use, damage or disruption of the school unit's computers, network, Internet services or other technology; any breach of security features; any failure to report a security breach; or misuse of computer passwords or accounts (the employee's or those of other users).

10. 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.

11. Employees should take special care to maintaining a professional and ethical digital footprint, and not engage in posting inappropriate photographs or defamatory content on the Internet. Staff must not use, access, create or distribute objectionable material such as jokes, stories or other material that is based on slurs or stereotypes, race, gender, ethnicity, nationality, religion or sexual orientation when using district computing devices.

C. Disclosure of Confidential Information

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

Email and other Internet communications mechanisms (including web sites, blogs and social networking sites) should not be considered secure or private. Communications with students or minors via email or other digital means must be for school related educational purposes only. Private use of social networking or other sites with students or other minors is strongly discouraged.

D. Employee/Volunteer Responsibility to Supervise Student Computer Use

Employees and volunteers who use school computers with students for instructional purposes have a duty of care to supervise such use and to enforce the school unit's policies and rules concerning student computer use. When, in the course of their duties, employees or volunteers become aware of a student violation, they are expected to stop the activity and inform the building administrator.

E. Compensation for Losses, Costs and/or Damages

An employee is responsible for compensating the school unit for any losses, costs or damages incurred by the school unit for violations of Board policies and school rules while the employee is using school unit computers or other technology, 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.

Isolated accidental damages to the school computing hardware will be repaired or replaced by the school unit. If damage is deemed not accidental or if there is a history of repeated damage by the employee, the unit may request compensation for repairs from those parties responsible.

Any damage or theft to school property must be reported immediately to the building administrator or director of information technology.

F. Additional Rules for Use of Privately-Owned Computers by Employee

1. An employee who wishes to use a privately-owned computing device in school must complete an Employee Request to Use Privately-Owned Computer form. The form must be signed by the employee, the building administrator/supervisor and the Technology Coordinator. There must be a legitimate work-related basis for any request.

2. The technology staff will determine whether an employee's privately-owned computer meets the school unit's network requirements.

3. Requests may be denied if it is determined that there is not a suitable work-related reason for the request and/or if the demands on the school unit's network or staff would be unreasonable.

4. The employee is responsible for proper care of his/her privately-owned computer, including any costs of repair, replacement or any modifications needed to use the computer at school.

5. The school unit is not responsible for damage, loss or theft of any privately-owned computer.

6. Employees are required to comply with all Board policies/procedures and school rules while using privately-owned computers at school.

7. Employees have no expectation of privacy in their use of a privately-owned computer while it is being used at school. The contents of the computer may be searched in accordance with applicable laws and policies.

8. The school unit may confiscate any privately-owned computer brought to school and used by an employee in school without authorization as required by these rules.

Cross Reference: GCSA – Employee Computer and Internet Use

First Reading: 3/3/10
Approved: 4/7/10
Revised: 4/6/11