

## **Policy GCSA-R - Employee and Volunteer Computer/Device and Internet Use Rules**

These rules provide general guidance concerning the use of the school unit's computers/devices and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by employees and volunteers. Each employee and volunteer is responsible for his/her actions and activities involving school unit computers/devices, network and Internet services, and for his/her computer files, passwords, and accounts. Employees and volunteers who have questions about whether a particular activity or use is prohibited are encouraged to contact the building administrator.

### **Access to School Computers/Devices and Acceptable Use**

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

### **Prohibited Uses**

Examples of unacceptable uses that are expressly prohibited include, but are not limited to, the following:

- a) Any use that is illegal or which violates Policy GCSA or other Board policies, procedures, or school rules, including harassing, discriminatory, threatening or bullying/cyberbullying 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/devices.
- b) Any attempt to access unauthorized websites or any attempt to disable or circumvent the school unit's filtering/blocking technology. Employees who believe filtering should be disabled or made less restrictive for their own temporary, bona fide research or other lawful purposes should discuss the matter with their building administrator.
- c) Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive, harmful to minors, or intended to appeal to prurient interests.
- d) Any communications with students or minors for non-school-related purposes;
- e) Downloading "apps" without prior authorization from the building administrator.
- f) Any use for private financial gain, commercial, advertising or solicitation purposes.
- g) Any sending of email or other messages to groups of school employees (except in the performance of their duties as school employees) without permission of the building administrator. Prohibited uses of the school's message systems also include but are not necessarily limited to:
  - i) Solicitation of membership in any non-school-sponsored organization;
  - ii) Advocacy or expression by or on behalf of individuals or non-school-sponsored organizations or associations;
  - iii) Raising funds for non-school-sponsored purposes, whether profit-making or non-for-profit;
  - iv) Selling articles or services of any kind, advertising or promoting any kind of business; or

- v) Any communications that represent an employee's views as those of the school unit or that could be misinterpreted as such.
- h) Sending mass e-mails or messages to school users or outside parties for any purpose without the permission of the building administrator.
- i) Any malicious use, damage or disruption of the school unit's computers/devices, network and Internet services; 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).
- j) Any attempt to delete, erase or otherwise conceal any information stored on a school computer/device that violates these rules or other Board policies or school rules, or refusing to return computers/devices or related equipment issued to the employee upon request.

### **C. Disclosure of Confidential Information**

Employees/volunteers are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential, and is not disclosed, used or disseminated without proper authorization.

### **D. Employee/Volunteer Responsibility to Supervise Student Computer/Device Use**

1. Employees and volunteers who use school computers/devices 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/device and Internet use. When, in the course of their duties, employees or volunteers become aware of a student violation or have a concern about student safety on the Internet, they are expected to stop the activity and inform the building administrator.
2. Any allowed student use of direct electronic communications must be closely monitored.

### **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/devices, 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/devices.

### **F. Employee Acknowledgment Required**

Each employee authorized to access the school unit's computers, networks and Internet services is required to sign an acknowledgment form (GCSA-E) stating that they have read policy GCSA and these rules. The acknowledgment form will be retained in the employee's personnel file.

### **G. Additional Rules for Use of Privately-Owned Computers/Devices by Employees**

1. The Principal or designee will determine whether an employee's privately-owned computer/device meets the school unit's network requirements.

2. 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.
3. The employee is responsible for proper care of his/her privately-owned computer/device, including any costs of repair, replacement or any modifications needed to use the computer/device at school.
4. The school unit is not responsible for damage, loss or theft of any privately- owned computer/device.
5. Employees are required to comply with all Board policies/procedures (including Sections A-C of these rules) and school rules while using privately-owned computers/devices at school.
6. Employees have no expectation of privacy in their use of a privately-owned computer/device while it is being used at school. The contents of the computer/device may be searched in accordance with applicable laws and policies.
7. The school unit may temporarily confiscate any privately-owned computer/device brought to school and used by an employee in school without authorization as required by these rules.

**Cross Reference:**

GCSA – Employee and Volunteer Use of School-Issued Computers, Devices and the Internet

First Reading: 08/17/15

Second Reading: 09/02/15

Adopted: 09/02/2015