CODE: GCSA - R

EMPLOYEE COMPUTER/DEVICES AND INTERNET USE RULES

Each Employee is responsible for their actions and activities involving school unit computers/devices, network and Internet services, and for their computer files, passwords and accounts. These rules provide general guidance concerning the use of the school unit's computer/devices, network and Internet services 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 the school unit's technology director.

A. Access to School Computers/Devices and Acceptable Use

The level of employee 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, network and Internet services is strictly prohibited.

All Board policies, school rules and expectations for professional conduct and communications apply when employees are using the school unit's computers/devices, network, and Internet services, whether in use at school or off school premises

B. Prohibited Use

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

1. Any use that is illegal or violates Policy GCSA and/or other Board policies/procedures, including harassing, discriminatory, threatening or bullying/cyberbullying communications and behavior, violations of copyright laws, or software laws etc. The school unit assumes no responsibility for illegal activities of employees while using school computers/devices, network and/or Internet services;

2. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive, harmful to minors, or intended for non-school related purposes;

1st Reading 08/10/09
Adopted: 09/15/09; Revised: 3/19/19
Reviewed by Committee: 10/26/21

3. Any communications with students or minors for non-school related purposes;

4. Any use for private financial gain, or commercial, advertising or solicitation purposes;

5. Any sending of email or other messages to groups of school employees (except in the performance of their duties as school employees) without authorization from the building administrator or Superintendent. Prohibited uses of school's message systems also include but are not necessarily limited to:

    a. Solicitation of membership in any non-school-sponsored organization;
    b. Advocacy or expression by or on behalf of individuals or non-school sponsored organizations or associations;
    c. Political or religious purposes;
    d. Raising funds for non-school sponsored purposes, whether profit-making or not-for-profit;
    e. Selling articles or services of any kind, advertising or promoting any kind of business; or
    f. Any communications that represent an employee's views as those of the school unit or that could be misinterpreted as such.

6. Downloading "apps" or using or encouraging students to use other online Educational software without permission from the Technology Director:

7. Opening or forwarding any e-mail attachments (executive files) from known sources and/or that are known to contain viruses;

8. Sending mass e-mails to school users or outside parties for school or non-school purposes without the permission of the Technology Director;

9. Any malicious use, damage or disruption of the school unit's computers/devices, networks 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);

1st Reading 08/10/09
Adopted: 09/15/09; Revised: 3/19/19
Reviewed by Committee: 10/26/21

10. Sharing passwords or other login information (except with authorized employees), using others passwords and/or login information, accessing or using other user's accounts; or attempting to circumvent network security systems;

11. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;

12. Using school computers, networks and Internet services after such access has been denied or revoked;

13. 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;

14. 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; and

15. Failure to comply with the school unit's record retention requirements for electronic records.

C. 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 expectation of privacy in their use of school computers, including e-mail messages and stored files.

D. 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 and is not disclosed, used or disseminated without proper authorization.

1st Reading 08/10/09
Adopted: 09/15/09; Revised: 3/19/19
Reviewed by Committee: 10/26/21

E. Employee/Volunteer Responsibility to Supervise Student Computer/Device Use

Employees and volunteers who use school computers/devices 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.

F. 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 related to violations of policies and/or rules while the employee is using school unit computers/devices, network, and/or Internet service, 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.

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

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

2. The Technology Director will determine whether an employee's privately-owned computer/device 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 their privately-owned computer/device, including any costs of repair, replacement or any modifications needed to use the computer/ device at school.

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

1st Reading 08/10/09
Adopted: 09/15/09; Revised: 3/19/19
Reviewed by Committee: 10/26/21

owned computer/device.

6. Employees are required to comply with all Board policies/procedures (including Sections A-F of these rules) and school rules while using privately-owned computers/devices at school.

7. Employees have no expectation of privacy in their use of 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.

8. 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.

H. Google G-Suite for Education

The School unit will, at its discretion, create Google G-Suite for Education accounts for eligible employees. Google G-Suite features will be enable on a user-by-user basis at the discretion of the Technology Director. Use of Google G-Suite is subject to Google's acceptable use policy (available upon request from the Technology Director), and all other school unit policies, procedures and rules. Employees must, at all times, take reasonable measures to protect files and information in G-Suite, including but not limited to, not sharing passwords and following all security and access rules.

I. Employee Acknowledgment Required

Any employees authorized to access the school unit's computers, networks and Internet services are 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.

1st Reading 08/10/09
Adopted: 09/15/09; Revised: 3/19/19
Reviewed by Committee: 10/26/21

1st Reading 08/10/09
Adopted: 09/15/09; Revised: 3/19/19
Reviewed by Committee: 10/26/21