



# WELLS-OGUNQUIT COMMUNITY SCHOOL DISTRICT

---

## **EMPLOYEE COMPUTER/DEVICE AND INTERNET USE RULES**

The intent of these School Committee rules is to provide employees with general requirements for utilizing the District's computers/devices, networks and Internet services. The School Committee rules may be supplemented by more specific administrative procedures and rules governing day-to-day management of an operation of the computer system.

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

Failure to comply with School Committee Policy GCSA, 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 Computers/Devices, Networks and Internet Services**

The level of access that employees have to District computers/devices, networks and Internet services is based upon specific employee job requirements and needs. Unauthorized access to secure areas of the District's computers/devices, network, and Internet services is strictly prohibited.

### **B. Acceptable Use**

Employee access to the school unit's computers/devices, networks and Internet services is provided for administrative, educational, communication and research purposes consistent with the District's educational mission, curriculum and instructional goals. General rules and expectations for professional behavior and communications apply to use of the District's computers/devices, networks and Internet services.

Employees are to utilize the District's computers/devices, networks and Internet services for school-related purposes and performance of job duties. Incidental personal use of school computers/devices 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.

### C. Prohibited Use

The employee is responsible for his/her actions and activities involving District computers/devices, networks and Internet services and for his/her computer files, passwords and accounts. General 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 Policy GCSA and/or other WOCSD School Committee policies, including harassing, discriminatory or threatening or bullying/cyberbullying communications and behavior, violations of copyright laws, or software licenses, etc. The District assumes no responsibility for illegal activities of employees while using District school computers/devices, network, and/or Internet service.
2. Any attempt to access unauthorized websites or any attempt to disable or circumvent the District'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.
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. Downloading "apps" or using or encouraging students to use other online educational services without prior authorization from the technology coordinator or building administrator.
5. Any use for private financial, commercial, advertising or solicitation purposes.
6. 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 the school's message systems also include, but are not necessary 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 District or that could be misinterpreted as such.
7. 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-supported organization; to solicit membership in or support of any non-school-sponsored organization; or 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.

8. Sending mass emails or messages to District/school users or outside parties for any purpose without the permission of the technology coordinator or building administrator.
9. Opening or forwarding any e-mail attachments (executable files) from unknown sources and/or that may contain viruses.
10. Sharing passwords or other login information (except with authorized school employees), using other users' passwords and/or login information, accessing or using other users' accounts or attempting to circumvent network security systems.
11. Any malicious use or disruption of the school unit's computers/devices, networks and Internet services or breach of security features; failing to report a known breach of computer security to the network coordinator
12. Any misuse or damage to District's computer/device equipment;
13. Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct;
14. Using school computers/devices, networks and Internet services after such access has been denied or revoked;
15. Any attempt to delete, erase or otherwise conceal any information stored on a school computer/devices that violates these rules or other School Committee policies or school rules, or refusing to return computers/devices or related equipment issued to the employee upon request.
16. Failure to comply with the District's record retention requirements for electronic records

D. Disclosure of Confidential Information

Employees are expected to use appropriate judgement 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.

E. No Expectation of Privacy

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

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

Teachers, staff members and volunteers who utilize school computers/devices for instructional purposes with students have a duty of care to supervise such use and to enforce the District's policies and rules concerning student use of school computer/devices and Internet use. When, in the course of their duties, employees/volunteers become aware of student violations, or have a concern about student safety on the Internet, they are expected to stop the activity and inform the building administrator.

G. Compensation for Losses, Costs and/or Damages

An employee is responsible for compensating the District for any losses, costs or damages incurred by the District for violations of School Committee policies and school rules while the employee is using District computers/devices, network, and/or Internet service, including the cost of investigating such violations. The District assumes no responsibility for any unauthorized charges or costs incurred by an employee while using District computers/devices.

---

**Cross-Reference:**      GCSA – *Employee Computer/Device and Internet Use*

**Approved** by Superintendent Richard A. Abramson:                      01/05/00  
**Revised** by the Wells-Ogunquit C.S.D. School Committee:                      11/13/19