# EMPLOYEE DEVICE AND INTERNET USE RULES

These rules implement Board policy GCSA (Employee Device and Internet Use). Each employee is responsible for his/her actions and activities involving School Department devices, networks and Internet services, and for his/her device files, passwords and accounts. These rules provide general guidance concerning use and examples of prohibited uses. These 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 Violations of Device and Internet Use Policy

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

B. Access to School Devices, Networks, and Internet Services

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

C. Acceptable Use

RSU 29 devices, networks, and Internet services are provided to employees for administrative, educational, communication, and research purposes consistent with the school unit's educational mission, curriculum, and instructional goals. All Board policies, school rules, and expectations for professional conduct and communication apply when employees are using the school unit's devices, networks, and Internet services.

D. Personal Use

School unit devices, network, and Internet services are provided for purposes related to school programs and operations, and performance of job responsibilities. Incidental personal use of school devices is permitted as long as such use: 1) does not interfere with the employee's job responsibilities and performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules, or any other Board policy, procedure, or school rules. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

E. Prohibited Uses

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

1. Any use that is illegal or which violates other Board policies, procedures, or school rules, including harassing, discriminatory or threatening communications and behavior, violations of copyright laws, etc., The school unit assumes no responsibility for illegal activities by staff while using school devices.

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, including commercial, advertising, or solicitation;

5. Any use as a forum for communicating by email 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 any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or non-profit. No employees 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.

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

7. Downloading or loading software or applications without permission 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 Superintendent or designee;

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

10. Any misuse or damage to the school unit's device equipment, including opening or forwarding email 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 device security to the system administrator;

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

14. Any attempt to delete, erase, or otherwise conceal any information stored on a school device that violates these rules or other Board policies or school rules.

15. Refusing to return devices issued to the employee upon request.

F. No Expectation of Privacy

RSU 29 devices remain under the control, custody and supervision of the school unit at all times. The school unit reserves the right to monitor all device and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school devices, including e-mail messages, or stored files, and internet logs.

G. 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.

H. Employee and Volunteer Responsibility to Supervise Student Use

Employees and volunteers who use school devices with students for instructional purposes 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 devices and Internet use and to enforce them. When, in the course of their duties, employees/volunteers become aware of a student violation, 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, or damages related to violations of Board policies and school rules while the employee is using school unit 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 devices.

J. Rules for Employee Use of Privately-Owned Devices

1. An employee who wishes to use a privately-owned device in school must submit a written request to the Technology Director to allow use of his/her privately-owned device. There must be a legitimate work-related basis for any request.

2. The Technology Director will determine whether an employee's privately-owned device meets the District's network requirements.

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

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

5. RSU 29 is not responsible for damage, loss or theft of any privately-owned device.

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

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

8. RSU 29 may confiscate any privately-owned device brought to school and used by an employee in school without the authorization required by Board policy and these rules.

Cross Reference: GCSA – Employee Computer and Internet Use
IJNDB – Student Computer and Internet Use
IJNDB-R – Student Computer and Internet Use Rules
JRA – Student Education Records and Information

Adopted: June 17, 2002

Revised: February 1, 2016