RSU #63

a. NEPN/NSBA Code: **GCSA**
b. Title: **Employee Use of School-Issued Computers, Devices, and the Internet**
c. Author:
d. Replaces Policy:
e. Date Approved: **01/23/2017 RSU #63**
f. Previously Approved: **02/29/2016**
g. Policy Expiration: **Review as Needed**
h. Responsible for Review: **Technology Committee/Policy Committee**
i. Date Reviewed: **03/13/2018 Technology Committee**
04/03/2018 Policy Committee
j. References:
k. Narrative:

Computers, networks, and Internet access are provided within RSU #63 (the District) to support the educational mission of the district and to enhance the curriculum and learning opportunities for students and school staff. This policy, and the accompanying rules, also applies to other school devices issued directly to staff (such as laptops and iPads) whether in use at school or off school premises. Employees are allowed to use privately owned computers at school with prior authorization, provided they comply with this policy and the accompanying rules.

I. Personal Use of District Computers: District computers/devices, networks, and Internet services are provided for purposes related to school programs, operations, and performance of employee job responsibilities. Incidental personal use of district computers/devices is permitted as long as such use:

A. Does not interfere with an employee's job responsibilities and performance;

B. Does not interfere with system operations or other system users; and

C. Does not violate this policy and the accompanying rules, any Board policy/procedure, or school rules.

"Incidental personal use" is defined as use by an individual employee for occasional personal communications that do not interfere or conflict with her/his job responsibilities.

II. Policy and Rules are Mandatory: Compliance with this policy and its accompanying rules concerning computer/device use is mandatory. An employee who violates this policy and/or any rules governing the use of District computers/devices will be subject to disciplinary action, up to and including termination. Illegal uses of District computers/devices will also result in referral to law enforcement.

III. Filtering Technology: The District utilizes Internet filtering technology designed to block access to child and adult pornography and materials considered obscene or harmful to minors.

IV. No Right to Privacy: The District computers/devices remain under the control, custody, and

supervision of the District at all times. The District reserves the right to monitor all computer/device and Internet activity by employees, whether on or off school premises. Employees have no expectation of privacy in their use of school computers/devices, network, and Internet services.

V. Notification of Policy and Rules: Employees will be informed of this policy and the accompanying rules through handbooks, the district website, and their understanding verified by a district-approved method.

VI. Implementation and Rules: The Superintendent or her/his designee is responsible for implementing this policy and the accompanying rules. Additional administrative procedures or rules governing the day-to-day management and operations of District computers/devices and network may be implemented, consistent with Board policies and rules.

VII. Employee Computer/Device and Internet Use Rules: Each employee is responsible for her/his actions and activities involving the District computers/devices, networks, and Internet services, and for her/his computer files, passwords, and accounts. These rules provide general guidance concerning the use of the District computers/devices 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 a building administrator or the Technology Coordinator.

A. Access to the District Computers/Devices and Acceptable Use

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

2. All Board policies, school rules, and expectations for professional conduct and communications apply when employees are using the District computers/devices, networks, and Internet services, whether in use at school or off school premises.

B. Prohibited Uses

The District assumes no responsibility for illegal activities while using its computers/devices. Examples of unacceptable uses of the District computers/devices that are expressly prohibited include, but are not limited to, the following:

1. Any use that is illegal or violates this policy and/or other Board policies, procedures, or school rules, including harassing, discriminatory, threatening, bullying/cyber bullying communications and behavior; violations of copyright laws, or software licenses; etc.

2. Any attempt to access unauthorized websites or any attempt to disable or circumvent the District filtering/blocking technology. Employees who believe filtering should be disabled or made less restrictive for their own

temporary, bona fide research, or other lawful purpose 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. Any communications with students or minors for non-school-related purposes.

5. Downloading "apps" without prior authorization from the Technology Coordinator or building administrator.

6. Any use for private financial gain, advertising, or solicitation purposes.

7. Any sending of email or other messages to groups of district employees (except in the performance of their duties as district employees) without the permission of the building administrator or Superintendent. Prohibited uses of the email system also include, but are not necessarily limited to:

a. Solicitation of membership in any non-district-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.

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

9. Sending mass emails to district users or outside parties for any purposes without the permission of the Technology Coordinator or building administrator.

10. Any malicious use, damage or disruption of the districts' 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).

11. Any attempt to delete, erase, or otherwise conceal any information stored on a district computer/device that violates these rules or other Board policies or school rules, or refusing to return computer/devices or related equipment issued to the employee upon request.

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 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 district computers with students for instructional purposes have a duty of care to supervise such use and to enforce the district's policies and rules concerning student computer 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 communication must be closely monitored.

E. Compensation for Losses, Costs, and Damages

An employee is responsible for compensating the District for any losses, costs, or damages incurred for violation of Board policies and/or school rules while the employee is using the District computers/devices, including the cost of investigation such violations. The District assumes no responsibility for any unauthorized charges or costs incurred by the employee while using the District computers.