Each employee is responsible for his/her actions and activities involving school unit technological resources (including but not limited to computing devices, network, internet services, and online services used by RSU #34), and for his/her files, passwords, and accounts. These rules provide general guidance concerning the use of the school unit's technological resources 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 IT Department.

The phrase "computing device" as used in this rule refers to all computing devices, including but not limited to desktops, laptops, tablets, internet-connected devices, and smartphones.

A. Access to School Unit Technological Resources and Acceptable Use

The level of employee access to school unit technological resources is based upon specific job requirements and needs. Unauthorized access to secure areas of the school unit's technological resources is strictly prohibited.

All Board policies, school rules, and expectations for professional conduct and communications apply when employees are using the school unit's technological resources, whether in use at school or off school premises.

B. Prohibited Uses

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

1. Any use that is illegal or which violates Policy GCSA and/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 technological resources.

2. Any attempt to access unauthorized web sites 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 make a request through the procedures established by the RSU #34 Technology Committee.

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

6. Any use as a forum for communicating with other school users or outside parties for:

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.

Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building administrator or the IT Department.

7. Sending mass communications (e.g., e-mails) to school users or outside parties for any purpose without the permission of the building administrator or IT. Sending mass communications (e.g., e-mails) to district users for any purpose without the permission of the Superintendent or IT Director.

8. Any malicious use, damage or disruption of the school unit's technological resources; any breach of security features; any failure to report a security breach; or misuse of passwords or accounts (the employee's or those of other users).

9. Any attempt to delete, erase, or otherwise conceal any information stored on a school technological resource that violates these rules or other Board policies or school rules, or refusing to return 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 Use

1. Employees and volunteers who use technological resources 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 technological resource use. When, in the course of their duties, employees or volunteers become aware of a student violation or have a concern about student safety, they are expected to stop the activity and inform the building administrator.

2. Any allowed student use of direct electronic communications should be 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 and school policies and rules while the employee is using school unit technological resources, 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 technological resources.

1. Staff members are responsible for the proper care of technological resources at all times, whether on or off school property, including costs associated with repairing or replacing the device if not covered by warranty. Staff shall be responsible for any costs associated with loss, theft, or damage to a device if the damage is deemed to be intentional, malicious, or due to negligence. This determination shall be made by the Superintendent following consultation with the IT Department. The decision of the Superintendent shall be final.

2. If a device is lost or stolen, this must be reported to the building administrator and the IT Department immediately. A report shall be made to the local police department immediately.

3. Devices must be returned in acceptable working order at the end of the school year or whenever requested by school or district administration.

F. Additional Rules for Use of Privately-Owned Computing Devices by Employee

An employee who wishes to use a privately-owned computing device (which shall include any device capable of connecting to the school network) in school must complete an Employee Request to Use Privately-Owned Computing 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.

The IT Department will determine whether an employee's privately-owned computing device meets the school unit's network requirements.

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

The school unit is not responsible for damage, loss, or theft of any privately-owned computing device. Employees are required to comply with all Board policies/procedures and school rules while using privately-owned computing devices at school.

Employees have no expectation of privacy in their use of a privately-owned computing device while it is being used at school. The contents of the computing device may be searched in accordance with applicable laws and policies. The school unit may confiscate any privately-owned computing device brought to school and used by an employee in school without authorization as required by these rules.

G. Other Rules

1. Staff members may be required to attend an informational meeting and sign acknowledgement forms before a computing device will be issued to them.

2. Violation of policies or rules governing the use of RSU #34 technological resources, or any careless use may result in, but is not limited to a staff member's computing device being confiscated and/or a staff member only being allowed to use the computing device on school grounds. The staff member may also be subject to disciplinary action for any violations of Board policies/procedures or school rules, up to and including termination.

3. The staff member to whom a computing device is assigned shall not loan it to others, and is responsible for its use.

Cross Reference: GCSA – Employee Computing device and Internet Use

First Reading: November 2016

Adopted: December 21, 2016