

Employee Digital Device and Internet Use Procedure

Each employee is responsible for their actions and activities involving RSU 40 computers/devices, network and Internet services, and for their computer files, passwords and accounts. These procedures provide general guidance concerning the use of RSU 40's computers/devices, network, and Internet services, and examples of prohibited uses. The procedures 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 Superintendent/designee.

Access to School Computers/Devices and Acceptable Use

The level of employee access to RSU 40 computers/devices, network and Internet services is based upon specific job requirements and needs. Unauthorized access to secure areas of RSU 40's computers/devices, network, and Internet services is strictly prohibited.

All Board policies, school procedures and expectations for professional conduct and communications apply when employees are using RSU 40's computers/devices, network and Internet services, whether in use at school or off school premises.

Prohibited Uses

Examples of unacceptable uses which are 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 procedures, including harassing, discriminatory, threatening or bullying/cyberbullying communications and behavior; violations of copyright laws or software licenses. RSU 40 assumes no responsibility for illegal activities of employees while using school computers/devices, network, and/or Internet service.
2. Any attempt to access unauthorized websites or any attempt to disable or circumvent RSU 40'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 the Superintendent/designee.
3. Any use involving materials that are obscene, pornographic, sexually explicit, sexually suggestive or harmful to minors.
4. Any communications with students or minors for non-school-related purposes.

5. Downloading “apps” or using or encouraging students to use other online educational services without prior authorization from the Director of Technology.
6. Any use for private financial, commercial, advertising or solicitation purposes.
7. Any sending of e-mail or other messages to groups of school employees (except in the performance of their duties as school employees) without authorization from the Superintendent/designee. Prohibited uses of the 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 RSU 40 or that could be misinterpreted as such.
8. Sending mass e-mails or messages to school users or outside parties for any purpose without the permission of the Superintendent/designee.
9. 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.
10. Any malicious use, damage or disruption of RSU 40’s computers/devices, network 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 school computer/device that violates these procedures or other Board policies or school procedures, or refusing to return computers/devices or related equipment issued to the employee upon request.
12. Failure to comply with RSU 40’s record retention requirements for electronic records.

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.

Employee/Volunteer Responsibility to Supervise Student Computer/Device Use

Employees and volunteers who use school computers/devices with students for instructional purposes have a duty of care to supervise such use and to enforce RSU 40's policies and procedures concerning student use of school computers/devices. 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.

1. Any allowed student use of interactive electronic communications must be closely monitored.

Compensation for Losses, Costs and/or Damages

An employee is responsible for compensating RSU 40 for any losses, costs or damages incurred by RSU 40 for violations of Board policies and school procedures while the employee is using RSU 40 computers/devices, network, and/or Internet service, including the cost of investigating such violations. RSU 40 assumes no responsibility for any unauthorized charges or costs incurred by an employee while using RSU 40 computers/devices.

Additional Procedures 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 Director of Technology. There must be a legitimate work-related basis for any request.
2. The Director of Technology will determine whether an employee's privately-owned computer/device meets RSU 40'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 RSU 40'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. RSU 40 is not responsible for damage, loss or theft of any privately-owned computer/device.
6. Employees are required to comply with all Board policies/procedures and school procedures while using privately-owned computers/devices at school.
7. Employees have no expectation of privacy in their use of a 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. RSU 40 may temporarily confiscate any privately-owned computer/device brought to school and used by an employee in school without authorization as required by these procedures.

Google G-Suite for Education

RSU 40 will, at its discretion, create Google G-Suite for Education accounts for eligible employees. Google G-Suite features will be enabled on a user-by-user-basis at the discretion of the Director of Technology. Use of Google G-Suite is subject to Google's acceptable use policy available upon request from the Director of Technology, and all other RSU 40 policies and procedures. 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 procedures.

Cross Reference: GCSA – Employee Computer and Internet Use

This is a required policy.

Adopted: October 2, 2008

Revised: October 3, 2013
Reviewed: September 11, 2013
Revised: March 21, 2019