Employee Digital Device and Internet Use Procedure

Each employee is responsible for his/her actions and activities involving RSU 40/MSAD 40 (District) digital devices, networks and Internet services, and for the employee's digital files, passwords and accounts. These rules provide general guidance concerning the use of the District's digital devices 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 Director of Technology.

A. **Consequences for Violation of Digital Device Use Policy and Rules** - Failure to comply with Board policy GCSA, these rules and/or other procedures and rules governing computer use may result in disciplinary action, up to and including termination. Use of the District's digital devises for illegal activities will also result in referral to law enforcement.

B. **Access to District Digital Devices, Networks and Internet Services** - The level of employee access to the District's digital devices, networks and Internet services is based upon specific job requirements and needs. Unauthorized access to secure areas of the District's digital devices and networks is strictly prohibited.

C. **Acceptable Use** - RSU 40/MSAD 40's digital devices, networks and Internet services are provided to employees for administrative, educational, communication and research purposes consistent with the District's educational mission, curriculum and instructional goals. All Board policies, District rules and expectations for professional conduct and communications apply when employees are using the District's digital devices, networks and Internet services, whether in use at District or off District premises.

D. **Personal Use** - District digital devices, networks and Internet services exist for purposes related to District programs and operations, and performance of job responsibilities. The Board acknowledges that incidental personal use may occur and reserves the right to define and enforce the limitations of such use by employees using the following guidelines: 1) it does not interfere with the employee's job responsibilities and performance; 2) it does not interfere with system operations or other system users; and 3) it does not violate this policy and Complaints involving the acceptable use of District computers, network and Internet services may be subject to review by the Superintendent, Board and Director of Technology for validity in accordance with policy and rules.

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 Board policies, procedures or rules, including harassing, discriminatory or threatening communications and behavior; violations of copyright laws, etc. The District assumes no responsibility for illegal activities of employees while using District digital 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, commercial advertising or solicitation purposes.

5. Any use as a forum for communicating with other District users or outside parties to solicit, proselytize, advocate or communicate the views of an individual or non-District sponsored organization; to solicit membership in or support of any non-District sponsored organization or to raise funds for any non-District sponsored purpose, whether profit or not-for-profit. No employee shall knowingly provide District e-mail addresses to outside parties whose intent is to communicate with District employees, students and/or their families. 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 District or that 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 District assumes no responsibility for illegal software copying by employees.

8. Sending mass e-mails to District users or outside parties for District or non-District purposes without the permission of the Technology Coordinator or building administrator.

9. Any malicious use or disruption of the District's digital devices, networks and Internet services; any breach of security features; or misuse of digital passwords or accounts (the employee's or those of other users).

10. Any misuse or damage to the District's digital equipment, including opening or forwarding e-mail attachments from unknown sources that may contain viruses.

11. Any attempt to access unauthorized sites, 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.

12. Failing to report a breach of digital security to the system administrator.

13. Using District digital 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 District digital device that violates these rules or other Board policies or District rules, or refusing to return digital equipment issued to the employee upon request.

F. No Expectation of Privacy - The District's digital devices remain under the control, custody and supervision of the District at all times. The District reserves the right to monitor all computer and Internet activity by employees and other system users. Employees shall have no expectation of privacy in their use of District digital devices, including e-mail, stored files and Internet access 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/Volunteer Responsibility to Supervise Student Computer Use - Employees and volunteers who use District digital devices with students for instructional purposes have a duty to supervise such use. Teachers, staff members and volunteers are expected to be familiar with the District's policies and rules concerning student digital device and Internet use and to enforce them. When, in the course of their duties, employees or 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 District for any losses, costs or damages incurred by the District for violations of Board policies and District rules while the employee is using District digital devices, 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.

J. Additional Rules for Use of Privately-Owned Digital Devices by Employee

1. An employee who wishes to use a privately-owned digital device for work purposes must seek prior authorization from the technology coordinator and may be asked to complete an Employee Request to Use Privately-Owned Computer form. The form must be signed by the employee, the District principal or supervisor and the Technology Coordinator. There must be a legitimate work-related basis for any request.

2. The Technology Coordinator will determine whether an employee's privately-owned digital device meets the District'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 the District's network or staff would be unreasonable.

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

5. The District is not responsible for damage, loss or theft of any privately-owned digital device.

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

7. Employees shall have no expectation of privacy in their use of a privately-owned digital device while it is being used at District.

8. The District may confiscate any privately-owned digital device used by an employee in District without authorization as required by these rules. The contents of the computer may be searched in accordance with applicable laws and policies.

K. Use of District E-Mail and Other District Managed Accounts - Staff members, stipend positions, consultants, individuals providing specific learning services, and Board members may have access to District e-mail. District employees and other positions as described previously may have access to District accounts such as the Student Information System and various other supported programs and resources. When a person who has access, as defined above for both e-mail and other managed accounts, leaves the District, access to their District accounts will be removed immediately and deleted within 7 days. Employees who are not returning in the following year will have their access removed from all District managed accounts following their last workday instead of at the end of the contractual year. E-Mail accounts inactive for 365 days will be deleted systematically. Any exception to this policy must be approved by the Superintendent.

E-Mail messages will be systematically deleted 160 days from the originating date. Exception: conferences are set by default to expire in 60 days but may be adjusted. An archiving system is in place for long-term storage of messages. With the approval of the Superintendent, the technology team will determine the expiration time line.

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: October 15, 2015