

EMPLOYEE COMPUTER AND INTERNET USE RULES

These rules accompany Board policy GCSA (Employee Computer and Internet Use). Each employee is responsible for his/her actions and activities involving school unit computers, networks and Internet services, and for their computer files, passwords and accounts. These rules provide general guidance concerning the use of the school unit's computers 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 Director of Technology.

A. Consequences for Violation of Computer Use Policy and Rules

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

B. Access to School Computers, Networks, E-Mail, and Internet Services

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

C. Acceptable Use

Mt. Blue Regional School District's computers, 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 communications apply when employees are using the school unit's computers, networks and Internet services.

All school-related electronic communications with parents and/or students will be conducted through official district-provided services (ie, email, PowerSchool). Personal email accounts, social networking accounts, etc will not be used for school communications.

D. Personal Use

School unit computers, network, and Internet services are provided for purposes related to school programs and operations, and performance of their job responsibilities.

Incidental personal use of school computers 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 which 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 of employees while using school computers.
2. Any use involving materials that are profane, obscene, pornographic, sexually explicit or sexually suggestive.
3. Any inappropriate communications with students or minors.
4. Any use for private financial gain, or commercial, advertising or solicitation purposes.
5. Any use as a forum for communicating by e-mail 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 not-for-profit. No employee shall knowingly provide school email 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 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 school unit assumes no responsibility for illegal software copying by employees.
8. Sending mass emails to school users or outside parties for school or non-school purposes without the permission of the Director of Technology or building administrator.

9. Any malicious use or disruption of the school unit's computers, networks, and Internet services; any breach of security features; or misuse of computer passwords or accounts (the employee's or those of other users).
10. Any misuse or damage to the school unit's computer 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 computer security to the system administrator.
13. Using school computers, networks and Internet services after such access has been denied or revoked; and
14. Any attempt to delete, erase or otherwise conceal any information stored on a school computer that violates these rules or other Board policies or school rules, or refusing to return computer equipment issued to the employee upon request.

F. No Expectation of Privacy

Mt. Blue Regional School District computers remain under the control, custody and supervision of the school unit at all times. The school unit reserves the right to monitor all computer, email, and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school computers, 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 school computers with students for instructional purposes have a duty of care to supervise such use. Staff members and volunteers are expected to be familiar with the school unit's policies and rules concerning student computer 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 school unit for any losses, costs or damages incurred by the school unit for violations of Board policies and school rules while the employee is using school unit computers, 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 computers.

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

1. An employee who wishes to use a privately-owned computer in school must make the request in writing to the Director of Technology and the building principal. 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 meets the school 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 school district's network or staff would be unreasonable.
4. The employee is responsible for proper care of their privately-owned computer, including any costs of repair, replacement or modifications needed to use the computer at school.
5. The school district is not responsible for damage, loss, or theft of any privately owned computer.
6. Employees are required to comply with all Board policies, administrative procedures and school rules while using privately-owned computers at school.
7. Employees have no expectation of privacy in their use of a privately-owned computer while it is being used at school.
8. The school unit may confiscate any privately-owned computer used by an employee in school without authorization as required by these rules. The contents of the computer may be searched in accordance with applicable laws and policies.

Cross Reference: GCSA – Employee Computer and Internet Use

Adopted: June 13, 2000

Reviewed: January 22, 2002, May 4, 2009, December 5, 2023

Revised: February 28, 2006, October 13, 2009