# EMPLOYEE COMPUTER AND INTERNET USE RULES

Every M.S.A.D. #29 employee is responsible for his/her actions and activities involving School Department computers, networks and Internet services, and for his/her computer files, passwords and accounts. These rules provide general guidance concerning use and examples of prohibited uses. These rules do not attempt to describe every possible prohibited activity by employees. Employees who have questions regarding whether a particular activity or use is acceptable should contact the building principal or Technology Director.

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

A. Access to School Computers and Acceptable Use

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

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

B. Prohibited Uses

1. Any use that is illegal or in violation of policy GCSA and/or other Board policies or rules, including harassing, discriminatory or threatening communications and behavior, violations of copyright laws or software licenses, etc.. M.S.A.D. #29 assumes no responsibility employees' illegal activities when using District computers, networks or Internet services.

2. Any attempt to access unauthorized web sites or any attempt to disable or circumvent the School Department's filtering/blocking technology.

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 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 non-profit. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the building principal or Technology Director.

7. An y communication that represents an employee's personal views as those of M.S.A.D. #29, or which could be misinterpreted as such.

8. Sending mass e-mails to school users or outside parties for ~~school or~~ non-school purposes ~~for any purpose~~ without the permission of the Technology Director or building principal.

9. Any malicious use, damage or disruption of M.S.A.D. #29's computers, networks or Internet services; any breach of security features; any failure to report a security breach; or misuse of the employee's or other employees' computer or Internet passwords or accounts .

10. Any attempt to delete, erase or otherwise conceal any information stored on M.S.A.D. #29's computer or network that violates these rules or Board policies or school rules.

11. Refusal to return computer equipment issued to the employee when requested to do so.

C. No Expectation of Privacy

M.S.A.D. #29 retains control, custody and supervision of all computers, networks and Internet services owned or leased by the school unit. The school unit reserves the right to monitor all computer and Internet activity by employees and other system users. Employees have no expectation of privacy in their use of school computers, including e-mail messages and stored files.

D. Confidentiality of Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

E. Employee and Volunteer Responsibility to Supervise Student Use

Teachers, staff members and volunteers who utilize school computers for instructional purposes with students have a duty of care to supervise such use. Teachers, 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/volunteers become aware of student violations, they are expected to stop the activity and inform the building principal.

F. Compensation for Losses, Costs and/or Damages

The employee shall be responsible for any losses, costs or damages incurred by the school unit related to violations of policy GCSA and/or these rules while the employee is using M.S.A.D. #29 computers, networks or Internet services, including the cost of investigating such violations.

M.S.A.D. #29 assumes no responsibility for any unauthorized charges or costs incurred by an employee while using District computers, networks or Internet services.

G. Additional Rules for Employee Use of Privately-Owned Computers

1. An employee who wishes to use a privately-owned computer in school must submit a written request to use his/her privately-owned

computer. The form must be signed by the employee, the building principal or supervisor and the Technology Director. There must be a legitimate work-related basis for any request.

2. The Technology Director will determine whether an employee's privately-owned computer meets the District's network requirements.

3. Requests may be denied if it is determined that there is not a legitimate 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 the care of his/her privately-owned computer, including any costs of repair, replacement or any modifications needed to use the computer at school.

5. M.S.A.D. #29 is not responsible for damage, loss or theft of any privately-owned computer.

6. Employees are required to comply with all Board policies and 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. The contents of the computer may be searched in accordance with applicable laws and Board policies.

8. M.S.A.D. #29 may confiscate any privately-owned computer brought to school and used by an employee in school without the authorization required by Board policy and these rules.

H. Employee Acknowledgment Required

Each employee authorized to access the school unit's computers, networks and Internet services is required to sign an acknowledgment form stating that they have read this policy and the accompanying rules.

Cross Reference: GCSA – Employee Computer and Internet Use
IJNDB – Student Computer and Internet Use



Cross Reference (cont.)

Adopted: June 17, 2002

Revised: May 6, 2013