

MONONA GROVE SCHOOL DISTRICT

Board Policy 362.1

COMPUTER NETWORK USE (Students)

The Monona Grove School District offers students access to school computer networks and the Internet. The Internet gives students access to educational resources around the world. Many classes incorporate the Internet as a primary research resource.

Students and parents/guardians are advised that a student's use of a school computer network – including which computers they use, which Internet sites they visit, what E-mail they send and receive and what material they save on the network – shall be monitored and sometimes accessed. Students should not expect privacy in any work they do, any communication they make or any material they save.

Students are responsible for good behavior while using school computer networks just as they are in a classroom or school hallway. In general, school rules for behavior and communications apply to computer use as well.

The use of school computer networks is a privilege, not a right. Failure to abide by the rules governing student computer use may result in a forfeiture of that privilege. The rules listed below provide specific examples of inappropriate and prohibited conduct, but these examples are not intended to be comprehensive.

1. All use of a school computer network must support learning appropriate for school.
2. No student may use a school computer network unless a supervising adult is in the same room.
3. No student without an active user account may use a school computer network and no student may log onto the system using someone else's account, even with his/her permission.
4. A student should primarily use E-mail as part of curricular-based classroom activities under the supervision of a staff member or volunteer.
5. No student may agree to meet with someone he/she has "met" online without parent/guardian approval.
6. No student may share personal information about himself/herself or others on the Internet, including personal passwords, full names, addresses, phone numbers, social security numbers or credit card information.

7. Students may subscribe only to high-quality discussion group mail lists that are approved by a teacher or other professional staff member, meet specific curriculum objectives and are consistent with district curriculum guides.
8. No student may access or attempt to access any material stored in another user's designated network storage space. No student may access or attempt to access material that is not available using his/her system name and password. No student may access or attempt to access unauthorized areas of the system. No student may access or attempt to access any other user's password.
9. No student may use a school computer network in such a way as to disrupt or threaten to disrupt the ability of others to use the system. Disruption may but need not include damage to equipment or stored data.
10. No student may use a school computer network to send threatening, hateful, harassing, insulting, defamatory or offensive communication.
11. No student may use a school computer network to obtain or transmit any material that advocates illegal acts or is defamatory, inaccurate, obscene, child pornography, harmful to minors or otherwise inappropriate.
12. No student may waste limited network resources, including bandwidth and storage space.
13. No student may download software.
14. No student may use a school computer network for illegal or commercial purpose.

Students suspected of inappropriate or prohibited computer use shall be investigated. Students found to have violated the rules above or other school rules governing behavior or communication may lose computer privileges, even if this leaves them unable to complete required assignments. They might also be subject to other discipline including suspension and/or expulsion and/or criminal prosecution. Decisions about punishment, and whether to involve the police, shall be made by the building and district administrators.

Although there is a national consensus among educators that the benefits of Internet access outweigh the risks, parents/guardians need to know that because anyone can publish on the Internet, many Internet sites contain material that is illegal, defamatory, inaccurate, offensive, obscene, child pornography, harmful to minors or otherwise inappropriate. Although it is impossible to eliminate the risk that students might be exposed to such material, the district attempts to reduce a student's risk of exposure to such material by enforcing rules #2 and #11 above, electronically monitoring student computer network use so that students can be held accountable for Internet sites they have visited and filtering Internet traffic coming into its networks to restrict access to inappropriate sites

Despite these risk reducing policies, determined students might still be able to access inappropriate sites and the Monona Grove School District does not guarantee that such access

will be impossible on a school computer network. Ultimately, students are responsible for where they choose to go on the Internet. Parents/guardians who are concerned about risk to their child because of Internet access should contact their child's principal.

LEGAL REFERENCES: Sections 120.13(1) Wisconsin Statutes
943.70
947.0125
Children's Internet Protection Act
Neighborhood Children's Internet Protection Act

CROSS REFERENCE: Administrative Exhibit 362.1, Computer Network Use Contract
(Students)
Board Policy 411.12 – Bullying
Board Policy 411.1 – Student Harassment

BOARD APPROVAL: October 11, 2006