

Employee Internet Responsible Use Contract

(The following executes Board Policy 6081.10-6081.2)

Technology and Network Access

The Moscow School District provides a computer network system, software, and access to the Internet as part of its curriculum resources. The use of the District's technology resources is a privilege and not a right. All network users, including students, employees, faculty, administrators and patrons or guests, are expected to use network resources for purposes appropriate to an education environment, consistent with the Computers and Networks Policy 6081.10 and Internet Safety Policy 6081.20, and refrain from any use that is not consistent with Federal, State, local laws, and district policies, purposes, or objectives.

Users must understand that communications created, received or backed-up on the system are public documents. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum. *Courts have ruled that old messages may be subpoenaed.* Although the district does not routinely monitor all messages, it does have the authority, at any time, to inspect the contents of any District equipment, files, or mail on its system for any legitimate business, legal or disciplinary purpose. Email related to a student is considered part of an educational record. As long as an email message or any attachment related to a student is maintained on a computer or server, it constitutes an educational record and is subject to FERPA (Family Educational Rights and Privacy Act) until it is permanently deleted.

Expectations of Staff

Technology serves to assist staff in fulfilling their job responsibilities. The District expects staff members to use the technology and network services as tools for instruction and professional work and to attend technology training in order to be able to use it effectively. All staff members should serve as role models in this capacity. It is imperative that staff know and enforce the Internet Safety Policy and teach and supervise **responsible** use of technology in their area. Parents may request restricted use of the networks and Internet in writing.

- A. Implement procedures established by the Superintendent and designees (pursuant to the Children's Internet Protection Act (CIPA, 12-21-2000 and NCIPA, 10-28-2008) to maximize system safety and security and, to the extent practical, prevent inappropriate network usage, include, but are not limited to:
 1. "The prevention of user access to or transmission of, inappropriate material over its computer networks, via Internet, electronic mail, or other direct electronic communications;
 2. The prevention of unauthorized access and other unlawful online activity, such as hacking,
 3. The prevention of unauthorized on-line disclosure, use, and dissemination of personal information regarding minors, and
 4. The use or dissemination of personal identification information of minors."
 5. Students and parents are required to read and sign the Student Responsible Use Contract before students are allowed access to the network.
 6. Each student who receives a network account will receive instruction from a Moscow School District staff member pertaining to the proper and responsible use of the District's networks and the Internet.
- B. District staff is responsible for instructing students in:
 1. Use of appropriate strategies when using electronic mail, chat rooms, instant messaging and other forms of direct electronic communications to ensure their safety and security,
 2. Unauthorized access, including so-called "hacking" and other unlawful activities by minors online, such as vandalism and harassment,
 3. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors,
 4. Search strategies designed to restrict minor's access to materials harmful to minors (local standards prevail),

5. Copyright and plagiarism,
 6. Downloading files.
- C. District staff is responsible for supervising and monitoring students' online activities. An information literacy curriculum provides students with the understanding and skills needed to use electronic resources effectively, and in an appropriate and responsible manner. District staff is responsible for integrating the use of technology into curriculum activities.
- D. District staff may utilize defined procedures to temporarily disable filtering for "adults only" for "bona fide research or other lawful purpose" are in place. District network staff monitors and evaluates sites not currently categorized or that might be categorized incorrectly.

Guidelines for the use of district technology and network services

Staff May:

1. Use district-owned software.
2. Use the Internet and other network services efficiently and with discretion to conserve District resources.
3. Save work on a thumbdrive, a computer, or a server, and request additional server space for instructional projects.
4. Manage and delete personal files.
7. Use an email account provided by the District as needed.
8. Connect computers to a projection device and make appropriate setting changes.
9. Request technical support from their respective Building Tech Representative and the Technology Department.

Staff MAY NOT:

1. Allow student use of technology or network services without supervision.
2. Access or use others' accounts or passwords.
3. Share a network account or passwords with another person or leave an open file unattended or unsupervised.
4. Access or send material inappropriate to a K-12 setting.
5. Send or receive material that may be hurtful to another person or detrimental to the operation of a computer, software, or network.
6. Send or post personal information about themselves, or others.
7. Move technology equipment or software to another location without the prior consent of a Technology Department representative. (Network connections may be lost; inventory tracking is made more difficult.)
8. Tamper with, assemble, disassemble, connect, or disconnect technology or network equipment. Systems may be damaged. Personal laptops may not be connected to the network without consent.
9. Install, download, copy, or delete district software. A software approval process must be followed before staff may install, download, or delete instructional software. The intent is to facilitate seamless, stable, and compatible computer and network functioning within the limitations of existing hardware, software, operating systems, and the individual's technical proficiency.
10. Create or change configurations (alter IP network number assignments or performance configurations).
11. Access, modify, or delete files created by another user without their prior consent.
12. Plagiarize or break copyright or trademark law.
13. Use district technology or network services for personal, entertainment, political, or commercial purposes.

Note: Use of school technology for political lobbying or commercial business is against the law. However, some instances of personal use may be acceptable (email, CD's) when such use does not interfere with job responsibilities and does not compromise district resources. For example, audio and video transmissions, such as online radio or video may slow down network services (access to the Internet, email, library catalog, file servers, etc.) throughout the district. Access to these services without curricular justification during the school day might interfere with instruction and district data gathering activities. After school,

evening and weekend use probably would not. Making an airline reservation is acceptable; running a travel agency from the District is not. To conserve District resources, please use these online resources with discretion.

14. Install, copy, or knowingly infect a computer with a virus. **Note:** Other examples of inappropriate technology/network behavior will be considered on a case-by-case basis. District Technology Staff or Building Technology Representative may be exempt from some of the items listed.

Consequences of Irresponsible Use

The Technology Department will report inappropriate behaviors, violations, or complaints to the building principal or supervisor who will take appropriate disciplinary action. Consequences for individuals violating the Staff Responsible Use Policy vary depending on the nature and seriousness of the violation. Consequences might include discussion, disciplinary action (due process), and/or the involvement of law enforcement agencies.

Warranties/Indemnification

1. Signing this contract signifies that the employee has read the District's Computers and Networks and Internet Safety Policy and will take personal responsibility for adhering to those policies as well as the specific behaviors and procedures contained in this guide.
2. The District makes no warranties of any kind, whether expressed or implied, in connection with its provision of access to, and use of, its computer networks and the Internet provided under this Policy.
3. The District will not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any Staff member arising out of the use of the electronic network.
4. The Staff member takes full responsibility for his/her use and is responsible for any and all loss, costs or damages resulting from the use authorized under this agreement, including but not limited to any fees or charges incurred through purchases of goods or services by the user over the electronic network.

Each employee will be given a copy of this policy and procedure and will sign an acceptable use before establishing an account or continuing their use (August 26, 2002).

Authorization for Use of Computer Resources within the Moscow School District

As a user of the Moscow Schools computer network, I hereby agree to comply with the rules stated above, communicating over the network in a responsible fashion while honoring all relevant laws and restrictions.

Staff Name (Print): _____ **Date:** _____

Staff Signature: _____

Pursuant to the Child Internet Protection Action (**CIPA**, April 20, 2001) notice is hereby given that there are NO facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and may monitor messages.

The intent of this policy is to promote the safe and efficient use of District technology resources. While there is no intent to monitor staff email, it is possible that instances of inappropriate use may become apparent when technicians are servicing domain accounts, monitoring firewall, virtual private network, and/or filter effectiveness, or when asked by an administrator to analyze students' use of the system. Any transgressions identified during a network analysis will be reported to the appropriate building administrator. Messages relating to or in support of illegal activities will be reported to the appropriate authorities. The District reserves the right to log network use including, but not limited to, particular web sites visited, files saved on the district network, computers and programs used, and fileserver space utilization. The District assumes no responsibility or liability for files deleted due to violation of fileserver space allotments or any other reason. (3-26-02)