AUP- Existing Employees

MOORE PUBLIC SCHOOLS
ELECTRONIC NETWORK ACCEPTABLE USAGE POLICY

A. Purpose Statement.

School District No. 02 of Cleveland County , Oklahoma (the "District") offers its students and employees access to network resources (the "Network") that may include but not be limited to:

- network storage for files and communication
- email accounts for communication between district employees, patrons, and when applicable, students
- Internet access for research and presentation
- software programs for instructional and productivity purposes
- availability of hardware to access network resources

While these resources provide the District with a means to communicate and inform in an efficient manner, the opportunity exists for abuse. The purpose of this document is to provide a guide to proper legal and ethical usage for employees and students. All individuals, student or other, who seek access to the District's network technology resources must read and agree to comply with the following policy. This policy will be made available to individuals through the Internet and through the publication of a student handbook made available to all students.

B. Internet and Network Access

1. Network access by users within the District should be for educational purposes and should be consistent with the educational objectives of the District. While accessing the network resources of other organizations, users should adhere to that organization's rules and regulations. Any transmission of information that violates state and federal laws is prohibited. *Any attempt to gain access to restricted areas by hacking or through the use of acquired passwords may result in appropriate punishment and removal of network privileges.*
2. Parental Consent: The District has web-filtering software in place that blocks access to *visual depictions deemed "obscene," "child pornography," or "harmful to minors;"* most information that can be considered harmful; however, the Internet is a rapidly evolving environment, *and the district is constantly reviewing and analyzing websites for appropriate content.* and even with the most advanced technology, not all harmful information can be filtered. Furthermore, *while the terms "obscene," "child pornography," and "harmful to minors" are legally defined for the purposes of filtering,* the *personal* standard of what is considered harmful may vary from individual to individual. The District encourages parents to discuss standards of acceptability with their students in regard to Internet usage. The District believes that it is primarily the parents' responsibility to communicate what is acceptable to view with their students. For this reason, all parents must read and accept the District's acceptable use policy prior to their student gaining access to District network resources. Acceptance of this policy is not permanent, and the parents can voluntarily revoke their students' access at any time. Any attempt to by-pass web filtering systems is considered a violation of this policy. The District does seek to block all content that can be considered obscene, pornographic, and harmful to minors. The district also offers training to students and staff designed to educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.
3. Privilege of Use: Access to the Network is a privilege and can be revoked at any time for failure to comply with the standards set forth in this policy. Furthermore, depending on specific circumstances, District administration may choose to remove a user's access for behavior determined to be detrimental to the network resources. Users will be required to agree to the District's Network Acceptable Use policy each year prior to gaining access.
4. Inappropriate Use: Usage that may be considered inappropriate may include but not be limited to:
    a. Inappropriate language/images: Use of vulgar or explicit language or images and/or defamatory language is prohibited. Users should not partake in personal attacks or activities that focus on distressing another individual.
    b. Identity Protection: Users must not disclose private information such as username and password to anyone. *Users must not attempt to access the network by using another user's username and password. Unauthorized possession of others' usernames and passwords constitutes a violation of acceptable use.* Students must not provide personal contact information to others. Students must not use the Network to arrange meetings with people they met online, nor should they communicate with other online users without direction from instructional staff. In the case of students using the Internet to apply for academic opportunities, students must have direct adult supervision. Users should report any communication that they feel is inappropriate or makes them

supervision. Users should report any communication that they feel is inappropriate or makes them feel uncomfortable.

c. Electronic Mail: At this time students are not granted wide-spread access to email. If provided for curriculum purposes, all rules mentioned below apply. Email communications should not be considered private. All email is stored on the District's servers and can be accessed by District administrators. For this reason, email communication should be professional and appropriate. Users should not access home or personal email using the District's Network. Users should not needlessly tie up the Network by creating, forwarding, or replying to messages that do not comply with the District's educational objectives. Email should not be used for commercial or political purposes.
d. Bandwidth Issues: Through the provision of federally funded e-rate, the district is able to access the Network at speeds greater than otherwise attainable. Although access can seem to be unlimited, this is not the case. Downloading large files and sending large attachments can obstruct the District's access. For this reason, users should refrain from downloading large files. If downloading is a necessity, users should refrain from doing so during instructional hours. Students should not download anything without consent of District personnel.
e. Copyright: All copyright laws are assumed under the District's Network policy. All plagiarism policies otherwise in place for students are also assumed.
f. Hardware modifications: It is the goal of the district's technology staff to supply all tools that are necessary for users to conduct educational business. However, the technology staff must balance department resources with the needs of the District. For this reason, users are prohibited through network policies from installing most types of software. Users should assume that any software not directly related to the performance of one's duties or to the furtherance of academic achievement is prohibited. All pending software and hardware purchases must be approved by the Technology Department prior to purchase.
g. Storage: Users are provided with an "H" drive (storage folder) in which they may store work/education related files. "H" drive, in most cases, is synonymous with a user's My Document's folder. As with bandwidth, storage is free for the user; however, it is not free to the District and is limited. Users must not store any personal files, photos, or other non-work/school related files on their "H" drive, local hard drive, or other district storage device. Large files such as video and music files should not be stored unless specifically used for school-related purposes. Should such files be found on District resources, the user may be contacted to verify purpose. The file may be deleted if not for approved purposes. Users should make use of the H drive (storage folder) and store all files there. Any files stored on the local machine may be deleted due to routine maintenance or computer malfunction. Files stored on the Network are routinely backed up by technology personnel. The technology staff cannot be held responsible for files stored on the local machine. Files stored on any District equipment should not be considered private.
h. Personal Property: Users may not bring non-district supplied technology equipment and/or software to use with Network resources including printers, wireless equipment, scanners, and mp3 players. Once again, the technology staff must balance District resources, providing support for personal equipment frequently offsets the benefits that such equipment might provide. Exceptions to this may include:
    i. External storage drives are permitted at this time. However, due to ever-changing security concerns, this allowance may change or be revoked entirely. Files brought on storage drives and transferred to district hardware should be for school/work-related purposes. Drives can be accessed by district personnel should there be a security concern. The district provides remote storage access via Synergy and should be used accordingly.

    ii. Digital cameras which do not require software installation.

    iii. With written permission from the Superintendent, laptops may be permitted to access the network. It is a violation for any hardware to access district network resources without district permission.

i. Access from home: Certain aspects of the Network are accessible from home. The District does not support any personal equipment that is used to access the Network. All equipment is the responsibility of the user and all files that reside on the user's machine remain the sole property of the user. The District does not have access to the user's files or information.

5. Enforcement: Users will be required to access this policy via the Moore Public Schools website, check that he or she agrees to the terms and conditions set forth in its entirety, complete user information and submit the form electronically. In doing so the user agrees to abide by the Moore Public Schools Network Acceptable Use policy. In doing so the user agrees to abide by the Moore Public Schools Network Acceptable Use policy. The user acknowledges that any violation of this policy may result in access to Network resources being revoked and other applicable disciplinary action being taken subject to any other approved discipline policies put in place by the Moore Board of Education.

VIOLATIONS OF ANY OF THE ABOVE RULES AND REGULATIONS MAY RESULT IN A LOSS OF ACCESS BY THE USER ALONG WITH OTHER DISCIPLINARY AS WELL AS LEGAL ACTION.

Adopted Revised Revised Revised Revised Revised Revised

10/9/05 2/14/00 10/14/02 8/14/06 5/14/07 8/11/089 7/12/10 6/1/2011

ELECTRONIC SIGNATURE: As a user of the Moore Public Schools Internet connection, I hearby acknowledge that I have read the above rules, and I recognize that violation of the rules can result in loss of access, disciplinary action, and possible legal action.*

- ( ) Yes

EMPLOYEE OR OTHER USER FIRST NAME*

EMPLOYEE OR OTHER USER LAST NAME*

Please select your site(s) from the list.*

- [ ] Apple Creek Elementary
- [ ] Briarwood Elementary
- [ ] Broadmoore Elementary
- [ ] Bryant Elementary
- [ ] Central Elementary
- [ ] Earlywine Elementary
- [ ] Eastlake Elementary
- [ ] Fairview Elementary
- [ ] Fisher Elementary
- [ ] Heritage Trails Elementary
- [ ] Houchin Elementary
- [ ] Kelley Elementary
- [ ] Kingsgate Elementary
- [ ] Northmoor Elementary
- [ ] Oakridge Elementary
- [ ] Plaza Towers Elementary
- [ ] Red Oak Elementary
- [ ] Santa Fe Elementary
- [ ] Southgate Rippetoe Elementary
- [ ] Sky Ranch Elementary
- [ ] Sooner Elementary
- [ ] Wayland Bonds Elementary
- [ ] Winding Creek Elementary
- [ ] Brink Junior High
- [ ] Central Junior High
- [ ] Highland East Junior High
- [ ] Highland West Junior High
- [ ] Moore West Junior High
- [ ] Moore High School
- [ ] Southmoore High School
- [ ] Westmoore High School
- [ ] VISTA Academy
- [ ] ASC

- [ ] Technology
- [ ] Transportation
- [ ] Publications
- [ ] Warehouse
- [ ] Maintenance

What is your account status?*

- ( ) My account is active.
- ( ) I previously had an account but it is not active.

Done Cancel