Dover Public School's Internet-Electronic Network Policy

2020-2021

A. Purpose Statement

School District No.I-002 of Kingfisher County, Oklahoma (the "District") offers its students & 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, & 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. The District believes that it is primarily a 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.

B. Responsible Use Guidelines/Internet Safety Requirements

These procedures are written to support the Responsible Usage Policy of this district and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different from face-to face interactions. 1.

1. **Use of Personal Electronic Devices**
   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. In accordance with all district policies and procedures, students and staff may use personal electronic devices (e.g. laptops, mobile devices and ereaders) to further the educational and research mission of the district. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Gaming systems that have wifi capabilities, such as Game Boys and PSP are prohibited. The district is not financially liable for loss or damage of personal equipment or software.
2. **Network**
   The district network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (blogs, websites, collaboration software, social networking sites, wikis, etc.). The district reserves the right to prioritize the use of, and

access to, the network. All use of the network must support education and research and be consistent with the mission of the district. Authorized users of personal devices will log into the MPS Wireless network provided to ensure mandatory filtering CIPA requirements are being met. Moore Public Schools will not be held responsible for data charges incurred on personal devices.

3. **Acceptable Use of District Technology Resources include but are not limited to:**
    a. Creation of files, digital projects, videos, web pages & podcasts using network resources in support of education & research;
    b. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and Web pages that support education and research;
    c. With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
    d. Staff use of the network for incidental personal use in accordance with all district policies and procedures;
    e. Connection of personal electronic devices to district network will be limited to wireless portable devices that support education and research.
4. **Unacceptable Use of District Technology Resources includes but is not limited to:**
    a. Personal gain, commercial solicitation and compensation of any kind without permission or approval from the superintendent or designee;
    b. Actions that result in liability or cost incurred by the district;
    c. Downloading, installing and use of audio files, video files, games or other non-curricular approved applications (including shareware or freeware) without permission or approval from the Superintendent or designee;
    d. Support for or opposition to ballot measures, candidates and any other political activity;
    e. Hacking, cracking, vandalizing, the introduction of malware, viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools, and any other malicious intent to disrupt, damage, or harm district resources;
    f. Unauthorized access to other district computers, networks and information systems;
    g. Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
    h. Information that could endanger others (e.g., bomb construction, drug manufacturing) not related to educational objectives of our district;
    i. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material;
    j. Attaching unauthorized personal devices to the district network. Any such device will be confiscated and additional disciplinary action may be taken. The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, nondeliveries, mis-deliveries or service interruptions caused by his/her own negligence or any other errors or

omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

5. **Internet Safety: Personal Information and Inappropriate Content**
    a. Students and staff should not reveal personal information, including a home address and phone number on Websites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium;
    b. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
    c. No student pictures or names can be published on any public class, school or district website unless the appropriate permission has been obtained according to district policy; and
    d. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.
6. **Filtering and Monitoring**
    a. Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.
    b. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
    c. Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to district browser settings & any other techniques designed to evade filtering or enable the publication of inappropriate content);
    d. E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
    e. The district will provide appropriate adult supervision of Internet use.
    f. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
    g. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively. H. The district reserves the right to prioritize the use of, and access to, the network.
7. **CIPA UPDATE/Internet Safety Instruction**
    a. All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.
    b. Age appropriate materials will be made available for use across grade levels.

c. Training on online safety issues and materials implementation will be made available for administration, staff and families.

8. **Copyright**
   Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.
9. **Ownership of Work**
   All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the district, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

C. Network Security and Privacy

1. **Network Security**
   Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password. The following procedures are designed to safeguard network user accounts:
   A. Change passwords according to district policy;
   B. Do not use another user's account;
   C. Do not insert passwords into e-mail or other communications;
   D. If you write down your user account password, keep it in a secure location;
   E. Do not store passwords in a file without encryption;
   F. Do not use the "remember password" feature of Internet browsers; and
   G. Lock the screen or log off if leaving the computer.
2. **Student Data is Confidential**
   District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA) and Children's Online Privacy Protection Act. For further information please see student handbook concerning digital images and publishing student information.
3. **No Expectation of Privacy**
   The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:
   A. The network;
   B. User files and disk space utilization;
   C. User applications and bandwidth utilization;

D. User document files, folders, and electronic communications;
E. E-mail;
F. Internet access; and
G. Any and all information transmitted or received in connection with network and e-mail use. No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State and Federal Government.

4. **Archive and Backup**
   Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers regularly. Refer to the district retention policy for specific records retention requirements.

D. Disciplinary Action

All users of the district's electronic resources are required to comply with the district's policy and procedures in addition to the Moore Public School Electronic Responsible Use agreement Violation of any of the conditions of use explained in the district's user agreement and Responsible Use Policy or in these procedures would be cause for disciplinary action in accordance to disciplinary policy and/or revocation of network and computer access privileges and/or legal actions.

Student Name (Print): _____

Student Signature: _____

Date: _____

HOUR: _____

Parent Signature: _____