

MOON AREA SCHOOL DISTRICT

SECTION: PUPILS

TITLE: ELECTRONIC SYSTEMS
USAGE FOR STUDENTS

ADOPTED: October 12, 1999

REVISED: September 17, 2012

| 250. ELECTRONIC SYSTEMS USAGE FOR STUDENTS | |
|--|---|
| 1. Purpose | <p>The Moon Area School District has made great strides in technology in order to facilitate learning, teaching, and daily operations. The Moon Area School District provides access to local, wide, and regional area computer networks to enable students within the school district to access both local and Internet resources.</p> <p>For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.</p> |
| 2. Authority | <p>The electronic information available to students and staff does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or any information that is retrieved via the Internet.</p> <p>The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.</p> <p>The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district and outside users.</p> |
| Pol. 218 | <p>The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.</p> <p>Unless otherwise noted, all technology, including but not limited to hardware, software, and files on the network are considered the property of the Moon Area School District and may be subject to normal review and maintenance procedure. Electronic mail or fileserver storage may be provided for instructional use and operational convenience; electronic mailboxes and fileservers are not for storage of personal files. Access to personal (i.e., not provided by the school district) email is prohibited under circumstances wherein it interfere with classroom instruction.</p> |

| | |
|----------------------|---|
| | <p><u>Technology users must follow any rules posted in a lab area and all instructional directives of the classroom teacher or supervisor at all times.</u></p> |
| <p>3. Definition</p> | <p>The term technology used in this document may include but is not limited to computers, laptops, digital camcras, digital music players, scanners, projectors, and network servers. It includes any device that connects with other district resources via a wired or wireless connection, such as iPhones and other "smart phones" with wireless capability.</p> |
| <p>4. Guidelines</p> | <p>This agreement will be executed by the student and his/her parent/guardian initially upon entering the school district at any grade level (usually Kindergarten), then "renewed" once again in 2nd grade, then 6th grade and then one (1) final time in 9th grade. Student and his/her parent/guardian approval of this agreement must be renewed using this schedule to maintain access to the district's network services. A parent/guardian may withdraw approval at any time by informing the Director of Technology in writing.</p> <p>Moon Area School District technology is to be used only in a responsible and ethical manner. As a user of district technology, you are expected to abide by the following guidelines:</p> <p><u>Computer/Technology Hardware</u></p> <ol style="list-style-type: none"> 1. The intentional destruction of district technology hardware will be considered vandalism. Each student will be held responsible for the intentional alteration of a computer workstation that occurs while s/he is at a classroom or library station. If a user notices a problem upon arriving at a workstation, s/he should report immediately to the classroom supervisor. |
| <p>Pol. 218</p> | <ol style="list-style-type: none"> 2. Users are expected to limit their printing to that which is absolutely necessary. All materials printed on school district printers are subject to review by the classroom supervisor as to whether the material is appropriate. Unauthorized printing of materials will be subject to disciplinary action. Unauthorized printing to a networked printer will be subject to disciplinary action. <p><u>Computer Software</u></p> <p><i>Technology software has been purchased to supplement and enhance the educational curriculum. The Moon Area School District is committed to full compliance of all software licensing agreements.</i></p> <ol style="list-style-type: none"> 1. Only software licensed to the Moon Area School District may be installed or used. |

20 U.S.C.
Sec. 6777
47 U.S.C.
Sec. 254

2. No games are to be installed or played on the computers without permission of the classroom supervisor.
3. Intentionally altering the files and/or settings on technology hardware will be considered vandalism.
4. Unauthorized copying of district software will be considered theft.
5. The district reserves the right to restrict the material that you access or post through the system. The district exercises this right through the use of a content filtering software application.

User ID Numbers/Passwords

1. A student's User ID/password is not to be disclosed to any other student.
2. A student is responsible for any work or mischief occurring during a session logged in under the student's User ID/password regardless of who actually did the work. If the actual user is located, responsibility may be apportioned between the actual user and the student whose User ID/password was used to access the computer.
3. No student is to be logged in under another student's User ID/password. This will not be tolerated and will result in immediate suspension of computer privileges.
4. If a student believes any other person is using his/her User ID/password, the student is responsible for reporting that immediately to the supervising teacher and/or building principal who will then contact the Director of Technology to assign a new User ID/password.
5. In the event of a lost or forgotten User ID/password, a replacement should be obtained immediately from the supervising teacher.

Internet And Network Computing

1. All students are issued network User ID numbers and passwords; users are not reveal their password to anyone except a supervising teacher.
2. Users will access their own files only. Under no circumstances should users access, copy, or modify the files or data of another user. To do so is illegal and may be considered plagiarism.

| | |
|---|--|
| <p>SC 1303.1-A Pol. 218.9</p> | <ol style="list-style-type: none"> 3. Users may not use the network for commercial purposes, nor for any illegal activities exemplified by (but not limited to) copying or circulating copyrighted materials or writing messages that threaten, harass, frighten, intimidate, bully, cyberbully, or annoy others. 4. Users will not attempt to disrupt the network, destroy network files, access unauthorized services, or to circumvent security measures to gain unauthorized access to the district's network or any other network (i.e. hacking). 5. Users will not intentionally or knowingly circulate files that may corrupt the integrity of the network (e.g., viruses). 6. Users will not access areas that contain "obscene" materials or other inappropriate information. If such sites are accessed accidentally, the user is to exit immediately. 7. Due to the potential of viruses, files from the Internet are not to be downloaded into the system without the explicit permission of the instructor. 8. Users are reminded that files and communications on the network are not private. The district reserves the right to access files in the course of normal maintenance or when there is cause to suspect misuse of the system. |
| <p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p> | <ol style="list-style-type: none"> 9. For personal safety, users are not to reveal personal information (e.g., address, phone number, location) over the Internet. In addition, the network may not be used to access, use, disclose or disseminate personal identification information regarding other students or staff. Chat room use is prohibited and blocked by content filtering software. 10. Users will not plagiarize work found on the Internet. 11. Users will not impersonate another user or claim anonymity and pseudonyms. 12. Users may not use personal computers, PDAs, cell phones, or other personal technology to access the school district's intranet, Internet or any other electronic system unless approved by the Technology Director and/or designee. <p><u>Web Site</u></p> <ol style="list-style-type: none"> 1. For educational purposes, and under the supervision of a teacher, students may create a web page/site to be hosted on the district's web server (e.g., senior project). In such a case the student would be solely responsible for the creation and maintenance of that site. |

250. ELECTRONIC SYSTEMS USAGE FOR STUDENTS - Pg. 5

| | |
|--------------------------------------|--|
| | <p><u>Discipline</u></p> <ol style="list-style-type: none">1. Students must realize that using the school district's computer network is a privilege and not a right. Students are granted this privilege for learning purposes. School district staff may inspect any and all items, physical or virtual pertaining to Moon Area School District's computer system. Logs may be kept of all activity occurring on the network.2. There is no expectation of privacy in regard to any files and communications on the network.3. Any student who violates the Electronic Systems Usage Guidelines may be subject to the following disciplinary procedures:<ol style="list-style-type: none">a. Suspension of computer privileges.b. Detention.c. Suspension from school.d. Expulsion, including permanent removal from school.e. Referral to the criminal justice system. Section 3933 of the Pennsylvania Crimes Code makes it a felony of the third degree to access any computer system or network with the intent to interrupt the normal functioning of any organization. It is also a misdemeanor of the first degree to intentionally give a password or user identification number about a computer without prior authorization. |
| Pol. 218 Pol. 218.8 Pol. 218.8 | <p><u>Internet Safety Education CIPA Compliance</u></p> <ol style="list-style-type: none">1. The School Board establishes that any information that is obscene, child pornographic or harmful to minors, all as defined by the Children's Internet Protection Act (CIPA), is inappropriate for access by minors. The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms; and cyberbullying awareness and response. |
| 47 U.S.C. Sec. 254 | |

20 U.S.C.
Sec. 6777
47 U.S.C.
Sec. 254

2. The Director of Technology or designee shall be responsible for implementing technology and procedures to determine whether the school district's computers are being used for purposes prohibited by law or this policy. The procedure shall include but not be limited to:
 - a. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors, or determined inappropriate for use by minors by the Board.
 - b. Maintaining and securing a usage log.
 - c. Monitoring online activities of minors.

Cell Phone/Personal Technology Device Confiscation

The district has defined policy for the confiscation of student-owned cellular phones and other personal technology devices. This policy has been established for the protection of both students and staff.

If a district administrator, principal, or teacher witnesses or has substantial reason to believe a cell phone or other personal technology device has been used by a student for cheating or in violation of district policy or local rules, the following steps should be taken:

1. The staff member will ask the student to turn off the device and hand it to him/her. If the student refuses to comply, appropriate disciplinary action should be taken.
2. The staff member WILL NOT turn on the device or view its contents.
3. The student will be disciplined as appropriate for violation of use of the device.
4. The device will be transported to the office, where it will be placed in an envelope that is sealed, signed, and dated by the principal or designee.
5. If there is reason to believe the device has been used in a manner that violates state or federal law, the principal may turn the device over to the authorities in question. If there is no reason to suspect use in violation of state or federal law, the device will be stored at the school until a parent or legal guardian of the student retrieves it.

6. To retrieve the device, a parent or legal guardian of the student should come to the main office during school office hours for the convenience of parents/guardians, should their child's cell phone be confiscated. The school may ask the person to provide some form of identification and make a copy for its records.
7. The parent/guardian will be given the envelope. They will be required to open the envelope and record the date and time they received the device, along with their signature. The school will retain the envelope as evidence of the chain of custody of the device.

Supplementary Rules

Additional rules or guidelines may be established at the district, school or classroom level. These rules may supplement, but not contradict, the policies defined herein.

References:

School Code – 24 P.S. Sec. 1303.1-A

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

Board Policy – 218, 218.8, 218.9, 814

2016-2017 Electronic Systems Usage Agreement

To Be Completed by All Students:

Student Section:

Student Name: _____ Grade Level: _____

Name of School: _____

Homeroom/Advisor Base room number and teacher:

I have read the Moon Area School District's Electronic Systems Usage Guidelines. I agree to follow all of the guidelines listed in this agreement. I understand that if I violate any of these guidelines, my user account may be restricted or terminated and that I may also face disciplinary action deemed appropriate by the building principal based upon the school discipline code.

Student Signature: _____ Date: _____

Parent/Guardian Section:

I have read the Moon Area School District's Electronic Systems Usage Guidelines. I grant permission for my child to use the District's technology services and understand that disciplinary and/or legal action may be taken if my child violates any of the listed guidelines. I understand that the District and its personnel are not responsible for any damages that my child may cause or experience while using the network services, including the purchase of goods or services via the Internet or network. I have discussed these guidelines with my child as well as any other restrictions I wish to impose upon my child that are above and beyond the scope of these guidelines. I understand that the District uses a content filtering program to block student access to inappropriate material; however, this is not a guarantee that my child won't be exposed to inappropriate material, as no filtering software or fire wall is perfect.

Because I value the necessity of using technology to supplement the educational programs at Moon Area School District, I grant my child permission to receive technology services for Internet/Network/Computer access.

Parent/Guardian Signature: _____ Date: _____

Parent/Guardian Name (printed): _____