Book	Policy Manual
Section	800 Operations
Title	Usage of Internet, Computers and Network Resources
Number	815
Status	First Reading

Legal	2. 20 U.S.C. 6777
	3. 47 U.S.C. 254
	4. Pol. 218
	5. Pol. 218.8
	6. Pol. 317
	7. Pol. 103
	8. Pol. 103.1
	9. Pol. 104
	10. Pol. 248
	11. Pol. 348
	12. Pol. 218.9
	13. Pol. 218.2
	14. 24 P.S. 4604
	15. 24 P.S. 4610
	16. 47 CFR 54.520
	17. 24 P.S. 1303.1-A
	18. Pol. 814
	19. Pol. 250
	21. Pol. 707
	22. Pol. 708
	23. Pol. 332
	24. Pol. 830
	25. 17 U.S.C. 101 et seq
	26. Pol. 901
	27. 18 U.S.C. 2256
	28. 18 Pa. C.S.A. 5903
	29. 18 Pa. C.S.A. 6312
	30. 47 CFR 54.513
	24 P.S. 510
	24 P.S. 4601 et seq
	Pol. 220
Adopted	April 24, 2017

Purpose

The computers, Internet and network, as property of the Moon Area School District, belong ultimately to the residents of Moon and Crescent Townships. Though the amount of use and technological advances may eventually render such resources obsolete, proper care of the

district's computers, Internet and network may result in maximized useful life. The Board of School Directors, as elected officials, recognizes its responsibility for the management of the computers, Internet and network, including labs and equipment of the district in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration. Such recognition includes the acknowledgement that while the computers, Internet and network used in the district's instructional and operational programs exist primarily for the education of its students, they shall also present an important community resource.

The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. District technology resources means all technology owned, operated, and/or licensed by the District, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, accounts, routers, and networks, including the Internet.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities and developmental levels of students.

Definitions

The term child pornography is defined under both federal and state law.

Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:[27]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.[29]

The term harmful to minors is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:[2][3]

1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion;

2. Depicts, describes or represents in a patently offensive way with respect to what is

suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and

3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[28]

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and

3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

Obscene - any material or performance, if:[28]

1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and

3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[3]

Spam mail – an unnecessary or annoying chain email sent to a large number of recipients.

Authority

The availability of access to electronic information 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 for any information that is retrieved via the Internet.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.

The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right, but not the duty, to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.[4][5][6]

The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:[3]

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory.[7][8][9][10][11]
5. Bullying.[12]
6. Terroristic [13]

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.[14][2][3]

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.[14]

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.[15][2]

The District may decrypt and inspect encrypted internet traffic and communications to ensure compliance with this policy.

Delegation of Responsibility

The district shall make every effort to ensure that this resource is used responsibly by students and staff.

The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[14]

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of

this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Student and minor user agreements shall also be signed by a parent/guardian.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[2][3][16]

1. 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 with respect to use by minors, or determined inappropriate for use by minors by the Board.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors.

4. Alert building administrator if discovered.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate behavior, including:[3]

1. Interactions with other individuals on social networking websites and in chat rooms.

2. Cyberbullying awareness and response.[17][12]

3. Network accounts shall be used only by the authorized owner of the account for its approved purpose.
Students shall respect the privacy of other users on the system.

Guidelines

Safety

It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social

networking websites, etc.

Internet safety measures shall effectively address the following:[3][16]

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restriction of minors' access to materials harmful to them.

Prohibitions

Users are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Nonwork or nonschool related work.
4. Chat room use.
5. Product advertisement or political lobbying.
6. Bullying/Cyberbullying.[17][12]
7. Hate mail, discriminatory remarks and offensive or inflammatory communication.
8. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.[18]
9. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[19]
10. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
11. Inappropriate language or profanity.
12. Transmission of material likely to be offensive or objectionable to recipients, including spam mail.
13. Intentional obtaining or modifying of files, passwords, and data belonging to other users.

14. Impersonation of another user, anonymity, and pseudonyms.

15. Fraudulent copying, communications, or modification of materials in violation of copyright laws.[18]

16. Loading or using of unauthorized games, programs, files, or other electronic media.

17. Disruption of the work of other users.

18. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

19. Accessing the Internet, district computers or other network resources without the authorization of the Director of Technology or designee.

20. Disabling or bypassing the Internet blocking/filtering software without authorization.

21. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

22. Inappropriate add-ins used on District network.

Use of Computers in the School Setting

The following priorities shall apply for access to and utilization of district computer labs:

1. The school day shall include time for student computer literacy and application classes in all school buildings. All buildings shall contain at least one (1) computer lab dedicated primarily to such classes, which shall be available to classes for Computer Assisted Instruction, or CAI. Building administrators, in cooperation with the Computer Coordinator, shall develop schedules for CAI.

2. Teachers shall have access to the computer labs before and after the school day for school-related work. The Computer Coordinator shall schedule teacher in-service on an as-needed basis.

3. Recognized parent groups that exist to support the educational process may be given permission by the building principals to use the computer labs. Such use shall be allowed only after completion of appropriate training and with proper supervision.

4. The computer labs may be made available for instruction of parents/guardians whose children attend the resident school. Such instruction is to be provided by district personnel only. A lab fee shall be charged that includes compensation for instructors plus an hourly lab usage fee. This fee shall be set and reviewed by the Board as needed.

5. Nonprofit community groups may use the computer labs at the discretion of the Computer Coordinator and Central Office, in accordance with applicable law and regulations, district administrative regulations, rules and Board policy. District employees serving as instructors or supervisors, shall be compensated. When non-district personnel are used to instruct these classes, provision shall be made for the presence of a district employee as a network/lab supervisor. Payment of the district employee shall be at a

periodically established rate. The network/lab supervisor shall have direct experience in the management of the particular lab being used. A fee shall be charged to the user that includes compensation, district payroll contributions and fringe benefits for district employees, plus an hourly lab usage fee with a minimum of $1.50 per hour, or any part of an hour, per machine used. The use of each computer shall result in a minimum three (3) hour charge.[30][21]

Use of Computers Outside the School Setting

Computers located in laboratory settings may only be removed by designated employees assigned to a position directly related to the operation of the laboratory. Removal of equipment shall not interfere with any lab usage. The computer instructor must use this computer equipment for school curriculum and/or school management purposes. Any personal use is strictly prohibited.[22]

Lab computers and associated equipment shall be returned at least two (2) working days before any scheduled laboratory activities. The computer instructor shall assume all financial responsibility for repair or replacement of removed equipment. The computer instructor and the Computer Coordinator or building principal shall sign a Computer Equipment Loan Form for all checked out equipment. The Computer Coordinator shall examine and verify the condition of the returned equipment.

Employee Email Use

Employees shall be allowed to utilize email for occasional personal use during non-working hours, in accordance with applicable provisions of an administrative compensation plan, individual contract, collective bargaining agreement and Board policy.[23]

Use of Personal Electronic Devices

The use of personal electronic devices on the District network is permitted only on designated networks. When a user connects a personal electronic device to a District network or District technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a District-owned device were being utilized. Users who connect a personal electronic device to a District network explicitly waive any expectation of privacy in the content exchanged over the District technology resources.

Wide Area and Local Area Networks

The district network topology consists of a Local Area Network (LAN) in each of the school buildings and a Wide Area Network (WAN) that provides connections between each building for communications to district file and application servers. Our WAN is directly connected to an Internet Service Provider (ISP). The district technology department deploys district email, district website hosting and filtered access to the Internet. The WAN incorporates a firewall, email, Internet filter(s) and routers to restrict access to authorized users only. The district Director of Technology will manage and approve all access to the district network.

The district will utilize both an open and closed network environment, which shall both be accessible from inside of the district. The closed network may only be accessed by district-owned equipment. It allows filtered access to the Internet, as well as to district resources. The open network allows heavily filtered Internet access only.

Remote Access

The district Director of Technology will authorize remote access to the district wide area network on an as-needed basis. Access will be controlled, monitored and reported to ensure against violations of district electronic systems usage policies. Such access may be granted to third parties for the purpose of maintenance of various systems. Should access by a third party be required, a unique network domain account will be created for each individual requiring access.

The district will deploy monitoring tools to monitor remote access to the network. All unauthorized access will be reported to the district Director of Technology.

Computer accounts local to the machine may be created by district technology personnel if required. Such accounts are subject to the same requirements as network domain user accounts.

Network Servers

The district utilizes a number of file, application and database servers. Each server has a specific purpose that varies in the degree of importance to what data is stored or accessible on that server. Therefore, the protection measures of each server may vary.

In general, server access is controlled using Microsoft Windows Server operating system software, which provides access to control and user authentication to server information and network shares on an as-needed basis. Microsoft's Active Directory with group policy feature provides logical control to the network, server and computer levels. The district network technician manages the access control and user authentication under the direction of the Director of Technology.

All server system administrative accounts, including but not limited to database and automatic service accounts, are controlled and managed by the Director of Technology.

Network Domain Accounts

Network domain user accounts control access to all district systems. Such accounts can only be created or altered with the permission of the Personnel office.

Access to network domain accounts and some or all network resources can be suspended due to violation of policy, or at the discretion of the Superintendent, Assistant Superintendent or other district administrator. Network domain accounts and all information contained therein including, but not limited to, the user's home directory and email, will be deleted ninety (90) days following termination of employment or contract, unless granted permission by the Superintendent or designee.[19]

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Passwords

User passwords for access to district systems, including networks, devices, databases and nightly processes, shall be required, in accordance with the following:

1. Passwords used to access systems must be a minimum of eight (8) characters long.

2. Passwords used to access systems must contain at least one (1) alpha, one (1) numeric and one (1) special character.

3. Passwords used to access systems must be changed at least every ninety (90) days.

Users are required to choose passwords that are challenging and difficult for others to guess, but easy to remember without feeling compelled to write it down. Passwords must not be easily deducible words or characters such as the user's first or last name, spouse's name, name of pet, or any word found in a standard, English dictionary.

Users must not write down or otherwise record their passwords in readable form near the system to which the password pertains, unless secured. For example, a user must not write his/her network password on a note and tape it to his/her computer.

The display and printing of passwords must be masked, suppressed or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

Passwords must not be stored in plain text or in other readable forms in places where unauthorized parties might recover them, including, but not limited to: batch files; login scripts; computers without access control; terminal function keys; or in software macros.

Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks. This will prevent them from being disclosed to wire-tappers, technical staff who are reading systems logs, and other unauthorized parties.

Passwords secure an individual account on the system. Each account must be used only by the individual formally assigned to that account.

While the specific generation retention depends on the computer system, users on all systems are prohibited from reusing a password when prompted to change it by the system. System administrators and other users with similar access privileges are prohibited from using the same password on multiple systems.

Users must change system-generated passwords upon first login with the initial password. This applies both to passwords that are attached to a new user account and passwords that have been reset by an administrator.

Old passwords used to access systems will be archived for at least five (5) password generations. Any new password created by the user will be rejected by the system if it matches any of the archived passwords for that account.

After at least three (3) unsuccessful logon attempts, the user's system account will be locked. The user must then contact the district Help Desk to have the password reset.

Users must promptly notify the district Help Desk if they suspect or know that their password integrity has been compromised. The password must be immediately changed.

User Identification Numbers

An employee's user identification number, or ID, shall not be disclosed to any other person.

Employees shall be responsible for any work or mischief occurring during a session logged in under the employee's user ID, regardless of who actually did the work. If the actual user is located, responsibility may be apportioned between the actual user and the employee whose user ID was used to access the computer.

An employee shall not be logged in under another person's user ID. Violations shall result in immediate suspension of computer privileges.

If any employee suspects another person is using his/her user ID, the employee is responsible for immediately changing his/her password and reporting the incident to the Director of Technology.

In the event of a lost or forgotten user ID, a replacement should be immediately requested and obtained from the Director of Technology.

Critical Information

Additional security measures are required for access to district servers and file shares that contain critical information including, but not limited to student accounting, personnel or financial data. Access is limited by the user's employment position. The appropriate district administrator and district Director of Technology will determine the eligibility for access to this information.[24]

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.[25][18]

District Website

The district shall establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district website shall comply with this and other applicable district policies.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.

Employees shall be allowed to create and maintain web pages on the district website for district-related instructional and communication purposes.

For public relations purposes, the district may publish photographs of events and/or bestow honors, awards and/or credit to employees. Objections to such use shall be stated in writing and submitted to the public relations department.[26]

Standard for Handling of Computer System Activity Logs

To aid in error correction, forensic auditing and security breach investigations and related efforts, computer system activity log files will be maintained.

Computerized logs containing security relevant events must be retained for a period of ninety (90) days. During this period, such logs must be secured so that they cannot be modified and ensuring that only authorized persons can read them. These logs are important for error correction, forensic auditing and security breach investigations and related efforts. In the event of a security incident, the logs are to be maintained for a time period determined by the designated administrator or designee.

System logs and application logs resident on Internet-accessible systems must be moved, at least daily, to other machines that are not directly Internet-accessible.

System administrators must regularly review logs from all systems. Prompt reviews are intended to identify problems in need of remedial action, including security relevant events.

Systems handling confidential or private information must securely log all significant events. Audit trails are essential in order to trace information through systems, providing the ability to reconstruct the processing flow. Examples of events include, but are not limited to, the following:

1. Password guessing attempts.
2. Attempts to use privileges that have not been authorized.
3. Modifications to production application software.
4. Modifications to system software.
5. User session activity including user IDs, login date/time, logout date/time.
6. Production application start/stop times.
7. Additions and changes to the privileges of users.
8. System boot/restart times.
9. System configuration changes.
10. System errors and corrective actions taken.

11. User ID creation, deletion and privilege change activity.

12. Privileged commands such as so to root, run as, addition of domains, etc.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[14]

Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action and/or legal proceedings.[4][5][6]

Attachment 815-1 Elementary User Agreement
Attachment 815-2 Middle School/High School User Agreement
Attachment 815-3 MASD High School Laptop Insurance Notice
Attachment 815-4 Employee User Agreement

Policy No 815 - Letter to Parents.pdf (27 KB)
Policy No. 815 Attachment 815-1.pdf (19 KB)
Policy No 815 Attachment 815-2.pdf (37 KB)
Policy No 815 Attachment 815-4.pdf (19 KB)
Policy No 815 Attachment 815-3.pdf (86 KB)
Policy No 815 Laptop Collection Procedures.pdf (35 KB)
Policy No 815 Distribution of Laptops Letter.pdf (36 KB)

Last Modified by Lisa M Brown on October 19, 2017

MOON AREA SCHOOL DISTRICT

ADMINISTRATIVE OFFICES

8353 UNIVERSITY BOULEVARD • MOON TOWNSHIP PA 15108 • 412-264-9440 • WWW.MOONAREA.NET • FAX: 412-264-3268

Dear Parent/Guardian,

Please carefully read the Moon Area School District Policy 815 on Usage of Internet, Computers and Network Resources. The policy can be found on the district's website located at www.moonarea.net and navigate to "Attending MASD" and "District Forms."

After reading the policy, please sign the form indicating that you have read and understand the policy. Both the student and the parent must sign the Usage of Internet, Computers and Network Resources agreement confirming that you have read the guidelines and policies and agree to follow them. Please have your child return the signed form to his or her homeroom or advisor base teacher.

Thank you for your cooperation,

MASD Administration

Attachment 815-1

2017-2018 Moon Area School District Elementary Handbook

Please sign and return to your child's homeroom teacher. Your signature indicates that you are aware that the MASD guidelines and policies may be read through www.moonarea.net.

Directions to Locate the 2017-2018 Online Elementary Handbook: www.moonarea.net, Schools, Select your Child's Elementary Building, Parent Resources, 2017-2018 Elementary Handbook.

I have read the 2017-2018 Elementary Handbook on my child's elementary school website through www.moonarea.net, or I have asked my child's elementary school for a printed copy, and understand all outlined guidelines and policies.

Parent/Guardian Name *(printed)*: _____

Parent/Guardian Signature: _____

Student Name: _____

Homeroom Teacher: _____

Date: _____

Attachment 815-2

Usage of Internet, Computers and Network Resources Agreement

Policy can be located at www.moonarea.net, Attending MASD, District Forms

STUDENT SECTION *(to be completed by all students)*

Student Name: _____ Grade: _____

Name of School: _____

Homeroom/Advisor Base Room Number and Teacher: _____

I have read the Moon Area School District's Internet, Computers and Network Resources 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 Internet, Computers and Network Resources Guidelines which can be found on the District website. 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 students' 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/Computers/Network Resources access.

Parent/Guardian Signature: _____ Date: _____

Parent/Guardian Name *(printed)*: _____

MOON AREA HIGH SCHOOL

8353 UNIVERSITY BOULEVARD • MOON TOWNSHIP PA 15108 • 412-264-9440 • WWW.MOONAREA.NET • FAX: 412-264-1271

BARRY J. BALASKI
PRINCIPAL

DAVID GALLUP
ASSISTANT PRINCIPAL

JASON D'ALESIO
ASSISTANT PRINCIPAL

MOON AREA SCHOOL DISTRICT

Laptop Collection Procedures:

1. Students will return laptops according to grade level during History classes at the end of May (dates to be determined by principals)
2. Laptop will be scanned by tech department indicating their official return
3. A stamped receipt will be given to the students and duplicate copy kept on file as official record of return
4. Laptops will then receive a student sticker indicating the date of return and student information
5. A final list of students by grade level who have not returned their laptop will be made – those students will be placed on the obligation list
6. Once all of the laptops are collected they will be reimaged and cleaned – as they are completed a new sticker will be placed on them signaling the completion of the reimaging and cleaning process – this is to be completed by the end of July
7. Laptops will then be placed in alphabetical order according to grade level
8. The student sticker sheets from the end of year and ones from after cleaning will be compared for any discrepancies
9. Laptops will then be stored in the teacher faculty lounge downstairs until they are ready to be brought up to the LGI for summer grade level distribution
10. Laptops will be placed in alphabetical order in the LGI in advance in preparation for the scheduled summer distribution hours and ready for parent/student pickup
11. The district will issue the same laptop to students each year as they progress through the high school. Any exceptions to this will be discussed with individual students and/or their families.
12. Seniors will take their laptop with them when they graduate in accordance with the policy.

MOON AREA HIGH SCHOOL

8353 UNIVERSITY BOULEVARD • MOON TOWNSHIP PA 15108 • 412-264-9440 • WWW.MOONAREA.NET • FAX: 412-264-1271

BARRY J. BALASKI
PRINCIPAL

DAVID GALLUP
ASSISTANT PRINCIPAL

JASON D'ALESIO
ASSISTANT PRINCIPAL

MOON AREA SCHOOL DISTRICT

Dear Parent/Guardian:

In order to maximize instructional time during the beginning of the school year and to minimize disruptions, the expectation is that High School students will obtain a laptop before school starts so they are prepared for the first day of school.

Students who do not obtain the laptop during the scheduled distribution days will need to find time in their schedules to meet with a representative from the Technology Department during regular laptop repair hours.

Distribution of laptops will start Monday August 6th and continuing according to the schedule below. Be sure to bring in the Laptop Insurance Form with the $60 fee and the Moon Area Internet Usage Agreement Form. No laptop will be issued without all completed forms and money. Students receiving a Free/Reduced lunch will be exempt from the $60 fee.

The schedule for distribution of Laptops:

Freshmen Distribution
Monday August 6, 2018 - 8:00am – 12:00pm and 1:00pm – 3:00pm
Sophomore Distribution
Tuesday August 7, 2018 - 8:00am – 12:00pm and 1:00pm – 3:00pm
Junior Distribution
Wednesday August 8, 2018 - 8:00am – 12:00pm and 1:00pm – 3:00pm
Senior Distribution
Thursday August 9, 2018 - 8:00am – 12:00pm and 1:00pm – 3:00pm

Make-Up Laptop Distribution Day #1
Tuesday August 14, 2018 - 8:00am – 12:00pm
Make-Up Laptop Distribution Day #2
Wednesday August 15, 2018 - 8:00am – 12:00pm

*All needed forms can be located on the Moon Area website, www.moonarea.net

Barry J. Balaski
Principal

David Gallup
Assistant Principal

Jason D'Alesio
Assistant Principal

MOON AREA SCHOOL DISTRICT LAPTOP INSURANCE NOTICE

****Please Read This Entire Document****

Student Name:_____ Grade:_____

Student ID Number:_____

Responsibility:

- School district laptops are only signed out during the school year. All students must return their computer at the end of the school year. Laptops are reimaged, checked, and cleaned each summer in order to prepare for the new school year.
- I understand that in order for a student to be assigned a Moon Area School District issued laptop, families are **required** by the school district to purchase the Moon Area School District's insurance policy and return an Acceptable Use Policy Agreement. **The current cost of laptop insurance is $50**. Insurance premiums are to be paid **annually** at the time laptops are distributed to the student. Insurance premiums can be paid using a check (made out to Moon Area School District), money order, or cash. The insurance policy covers accidental damage, normal wear and tear, theft, and loss. Loss is defined as irreparable damage due to such things as: fire, flood, lightning or some other natural disaster. **Misplacement is not loss.**
    - **In order for a claim of loss to be "valid", the student and/or family must produce the remains of the computer for the district to determine if the machine is damaged beyond repair.**
    - **In order for a claim of theft to be "valid", the student and/or family must produce a police report within seven (7) school days of the occurrence.**
- Product failure is fully covered and is not the responsibility of the student, family, or school district. Moon Area School District and its affiliates are the only authorized parties who can classify a defect as product failure.
- I understand that repair and replacement costs associated with instances that are not covered by the school's insurance policy are the **sole financial responsibility of the students and families.** This includes but is not limited to; **intentional damage, negligent damage, misuse, and misplacement (detailed above).**
- I understand that assessment and classification of damages (accidental vs. intentional/misuse) are the sole responsibilities of the school district. All findings and determinations by the district final.
- Students and parents will be held responsible for proper use and care of the laptop, as is the case with all District - issued materials.
- Moon Area School District provides filtering for inappropriate websites/material. Parents/Guardians are responsible for monitoring their child's use of the laptop when at home to ensure they do not adjust the laptop's settings and preferences or view inappropriate websites/material.
- **Repairs to the laptop are to be made by authorized school district personnel.** Repairs may be made at any time a school official deems them necessary for the proper operation of the computer. Financial responsibility for computer repairs will be determined in accordance with the provisions of this agreement. When a student laptop is being repaired, a loaner laptop may be available. Students signing out a loaner laptop incur the same responsibility for the loaner as they would for their assigned laptop.
- This signed agreement is binding for the length of time the student possesses a Moon Area School District issued laptop. However, the district may opt to renew and/or revise this agreement on an annual basis.

Terms and Explanation of the District's Insurance Policy

This policy covers:

- Full replacement cost for loss or theft (regardless of the age of the computer) with a deductible to be paid by the insured party. Loss is defined as irreparable damage due to such things as: fire, flood, lightning or some other natural disaster. **Misplacement is not loss.**
- Accidental damage to the computer (as defined in this agreement) with a deductible to be paid by the insured party.

Deductible Schedule for Accidental Damage/Loss:		**Deductible Schedule for Theft:**	
First incident of accidental damage/loss	**$60.00**	**First theft**	**$100** ***(with police report)***
Second incident of accidental damage/loss	**$80.00**	**Subsequent theft - Full Replacement Cost**	
Third incident of accidental damage/loss	**$100.00**		
Subsequent incidents of accidental damage/loss	**$300.00**		

NOTE: Deductibles do not reset annually, they are cumulative for the duration of time a student is enrolled or re-enrolled in MAHS

This policy DOES NOT cover:

- Intentional damage and/or negligent damage to the computer (As determined solely by the Moon Area School District)
- Misplacement of the computer
- Misuse of the computer (i.e. careless liquid spills, defacing the computer with stickers, ink or paint or other materials, and/or carrying and handling the machine in an incorrect manner).
- With the exception of manufacturer defect, this policy does not cover theft, loss or damage (accidental or intentional) to the AC power adapter, or any other district issued accessories. It only covers the computer itself. Damage, theft, or loss of these parts is the sole financial responsibility of the students and their families.

Frequently Asked Questions

What are the most frequent accidental damages that occur to the student computers?

Some of the most frequent damages are cracked LCD screens, damage to the motherboard, damage to keyboards and damage to the outer plastic/aluminum casing. Full replacement cost of a computer is $500 - $800.00 depending on the make and model and the year replacement is required. Remember that costs reflect hardware, software, technical support, warranty, and maintenance.

What happens if my computer cannot be repaired?

In the event that a computer cannot be repaired a comparable or new computer will be assigned to the student, after every attempt to fix the existing computer has been exhausted. This assignment of a new or comparable computer will be at the discretion of the Moon Area Technology Department.

Are there any costs to students on free and/or reduced lunch?

The district will pay the cost for the insurance premium. The only cost that these students may incur is the deductible as described previously.

How do I make a claim under the MASD policy?

Within seven (7) school days, the student will submit a written report of the loss or damage to the main office (forms can be obtained in the office) and to the school resource officer who will investigate the incident if the claim is for theft or vandalism. If a deductible is required, this must also be paid in the form of cash or check to Moon Area School District. Once the report has been made, the deductible paid (if necessary) and the investigation is finished, the claims process is complete. For damage, the student will fill out and sign a Computer Repair Form as instructed to do so by district personnel. For theft, a copy of a police report must be submitted to the district.

Can my premium or deductible be increased? Can my premium be canceled?

It is the district's intention to provide comprehensive coverage for a minimal cost to the student; however, if claims become excessive, frequent, or a fraudulent claim is suspected, the district has the sole right to increase premiums or deductibles (see schedule above), or to cancel the insurance at any time.

Will students keep the same laptop throughout their senior year?

Students entering the 9th grade will be issued a new laptop. Students entering grades 10-12 that are new to Moon Area High School will be issued a computer that is comparable to those issued to the same grade. The same laptop will follow the student throughout their high school career. Students in grades 9-11 will turn in their laptop each summer to be cleaned, fixed, and reimaged according to the guidelines of this policy. At the end of their senior year, students will be given the opportunity to keep their laptop at no additional cost.

Insurance Selection (All Students and families must insure the computers.)

Having fully read this Moon Area Insurance Agreement, I understand my responsibilities for caring for and insuring the computer, and I agree to the terms above regarding the laptop computer my student will receive from the Moon Area School District.

Parent/Guardian Names(s) PRINT: _____ Grade:_____

Parent/Guardian Signature(s) _____ Date:_____

Student Signature _____ Date: _____

Attachment 815-4

Usage of Internet, Computers and Network Resources Agreement

Policy can be located at www.moonarea.net, Attending MASD, District Forms

EMPLOYEE SECTION *(to be completed by all employees)*

Printed Employee Name: _____

Job Title: _____

Name of School or Building: _____

I have read the Moon Area School District's Internet, Computers and Network Resources 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 face disciplinary action deemed appropriate by my supervisor and the MASD School Board based upon the school discipline code.

Employee Signature: _____ Date: _____