Book	Policy Manual
Section	200 Pupils
Title	Student Acceptable Use Of Computer Network Network System/Internet
Number	238
Status	Active
Legal	1. 20 U.S.C. 6777 2. 47 U.S.C. 254 3. 24 P.S. 1303.1-A 4. Pol. 249
Adopted	June 7, 2011
Last Revised	July 17, 2012

Purpose

The purpose of computer network use, including Internet access, shall be to support education and academic research in and among the schools in the East Lycoming School District by providing unique resources and the opportunity for collaborative work. Network facilities shall be used to support the district's curriculum and enhance communications and research capabilities for students, teachers, administrators, and support staff.

The East Lycoming School District ("District") has established the East Lycoming School District Technology Network ("System"). The System provides opportunities for communication: (1) within the school district; (2) outside the school district among educational and non-educational entities; and (3) through worldwide resources such as the internet. The System includes but is not limited to any District-owned, leased or licensed or user- owned personal hardware, software, or other technology used on school district premises or at school district events, or connected to the school district network, containing school district programs or school district student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a computer.

The Internet is a worldwide collection of computer networks, connecting millions of computers in nearly every country. Access to the System allows the user to participate in a variety of efficient and educationally valuable learning experiences through the Internet; however, students in the East Lycoming School District will be limited to using the Internet to support the District curriculum, policies, and mission statement.

Definitions

"Bandwidth" – a measure of available or consumed data communication resources.

"Bandwidth intensive application" – any application which may cause a general slowdown of computer function.

"Executable files" – files in a format that a computer can directly execute. This includes but is not limited to files stored on a flash drive which, when the flash drive is connected to a computer, the computer can access and run directly from the flash drive without needing the files to be downloaded directly onto the computer's hard drive.

"Fair use" – the limited use of copyrighted material without the need for permission from the rights holder, such as use for scholarship or review.

Authority

The use of network resources, including the Internet, is a privilege, not a right; inappropriate use will result in the cancellation of these privileges and/or appropriate disciplinary action. All student network users must complete and sign an acceptable use agreement that indicates that they understand and will abide by the provisions of this policy.

The district reserves the right to log network use and to monitor fileserver space utilization by district users. Users should not expect or assume any right of privacy with respect to the System. Routine maintenance and monitoring of the System may lead to the discovery of a potential violation or misuse of the System. System administrators may access or examine files or accounts that are suspected of unauthorized use or misuse. Searches will be reasonable and in the context of the alleged violation. Communications, access logs, and other System records may also be subject to search by outside parties upon a court order. An authorized system administrator may remove or alter any necessary file that threaten to interfere with the operation of the System or that violates some portion of this agreement. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the System.

The District is under no obligation to support personal devices or computers on the premises, and shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The District shall not be held liable for the loss of student created files. Student network files will be deleted at the conclusion of each school year.

District technology and technology services depend on finite resources such as bandwidth and server storage. All users will be expected to maintain their files and access to services in a manner that is conducive to efficient resource allocation. Users are expected to monitor the number and size of files stored on computers and the network, and delete old or unnecessary files. Bandwidth intensive applications should be kept to a minimum.

All users must make reasonable efforts to protect against theft or damage of district equipment. Personal laptops left unattended must be secured to a desk or other fixture with a laptop lock, or locked in a cabinet or locker.

Delegation of Responsibility

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

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, pornographic, or harmful to minors, or determined inappropriate for use by minors, according to the provisions of this policy.

2. Maintaining and securing a usage log.[1][2]

3. Monitoring online activities of minors.

Guidelines

Acceptable Use

Acceptable use of the System must support education and academic research consistent with the mission and educational goals of the school district. Use of network and computer resources must comply with rules appropriate for that network. Network accounts are to be used only by the authorized owner of the account for authorized purposes.

The determination as to whether a use is appropriate lies solely within the discretion of the school district.

Prohibited Uses

Students are expected to act in a responsible, ethical, and legal manner in accordance with district policy, accepted rules of network etiquette, and State and Federal law. The use of the computer network System for illegal, inappropriate, or unethical purposes by students is prohibited. Specific prohibited uses of the System include, but are not limited to, the following:

1. Commercial, political lobbying, illegal activity, and product advertisement.
2. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
3. Fraudulent copying, communications, or modification of materials in violation of copyright laws. This includes duplicating material from the Internet that could not be considered Fair Use for education purposes without permission from the creator unless permission is so stated. Users that violate copyright laws will be solely responsible for such violations.
4. Inappropriate language or profanity on the network and transmitting material likely to be offensive or objectionable to recipients. This includes Bullying/CyberBullying.[3][4]
5. Intentionally obtaining or modifying files, passwords, and data belonging to other users. This includes reading, executing, changing, or deleting any file belonging to someone else without permission from the owner.
6. Destruction, modification, abuse or unauthorized access of System hardware, software, and files; using approved district software or internet solutions to mask prohibited activities.
7. Using software, altering proxy settings, or using any other means to bypass district content filtering or network security settings.
8. Impersonating another user, anonymity, and use of pseudonyms.
9. Loading or use of unauthorized games, programs, files, or other electronic media
10. Installing software on computers without proper license and approval of the technology department.
11. Intentionally or negligently using computing resources in such a manner as to cause congestion and performance degradation of the System or disruption of the work of other users.
12. Plagiarizing the work of others.
13. Copying or sharing files with other students and submitting it as individual work.
14. Altering or tampering with a computer, either hardware or software.
15. Attempting to repair, alter, or relocate hardware without the approval of the technology department.
16. Personal file storage and archiving.
17. Hacking, i.e., attempting to access and/or modify a computer's operating system without authorization, to attempt to uncover security loopholes or data protection schemes.
18. Connecting any devices or personal computers to the System without the approval of the technology department. USB flash drives are an approved device and do not require preapproval of the technology department. The use of these drives is the only permitted method for transferring school related files between home and school. No executable files shall be run from a

flash drive.

19. Saving executable files on any network drive or directory.

20. Personal entertainment, web browsing or "surfing" unrelated to learning goals during school hours.

21. Use of the System for social networking and/or communicating with individuals outside of the District is generally not permitted. Absent administrative approval, any access of sites used for social networking, chat, e-mail, and forums, is prohibited. If approved, all such communications must occur within the time frame and physical location established by the requesting teacher. Approval of such sites and/or communications shall be documented and granted only by both the appropriate building principal and the district technology coordinator with said approval not granted beyond the school year.

22. Using the System in a way that violates other district policy, applicable law, or regulation that subjects the District to liability.

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, the following procedures shall be followed:

1. Students shall not reveal their passwords to another individual.

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

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

Safety

Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.

To the greatest extent possible, student users of the network will be protected from harassment of unwanted or unsolicited communication.

1. Any student who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator.

2. Students shall not reveal personal addresses or telephone numbers to other users on the network, including chat rooms, e-mail, Internet, etc.

To the extent possible, Internet safety measures shall address the following:

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.

2. Safety and security of minors when using computer network resources.

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 minor's access to materials harmful to them.

6. The district will educate all students about the appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms, and Cyberbullying awareness and response.

Consequences for Inappropriate and/or Unacceptable Use

Students shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Students may be disciplined for unauthorized or illegal use of, or access to, computers, software, telecommunications, and related technologies for any willful act that causes physical, financial, or other harm, or otherwise disrupts information technology.

Failure to follow the procedures and prohibited uses listed in this policy may result in loss of network access. Other appropriate disciplinary action may also be instituted in accordance with school district policies as well as State and Federal statutes, even if acts are committed away from school property and outside school hours.

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