Book	Policy Manual
Section	800 Operations
Title	Internet Access
Code	815
Status	Active
Adopted	September 18, 2001
Last Revised	December 19, 2017

Purpose

The Tamaqua Area School District will provide access to the Internet for students with their parents'/guardians' consent and for staff members to locate material to meet their educational and personal information needs. School library media specialists and teachers will work together to help students develop the critical thinking skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet educational goals that are consistent with the school district's Strategic Plan.

Connectivity to the network through school resources is a privilege, not a right, and may be revoked for anyone who uses these resources inappropriately as determined by school district authorities.

Authority

Due to the nature of the Internet as a global network, connecting thousands of computers around the world, inappropriate materials, pornography and obscenity can be accessed through the network. In accordance with the Children's Internet Protection Act (CIPA), Tamaqua Area School District utilizes technology protection measures to block and filter inappropriate materials. The Tamaqua Area School District cannot, however, completely block access to these resources because of the nature of the technology that allows the Internet to operate. Accessing these and similar types of resources or transmitting such resources will result in suspension or other disciplinary measures in accordance with other district policies. Through a program of education, the school district will educate students and staff about their individual responsibility to refrain from engaging in this and other unacceptable uses of the network, and as to the consequences of their actions if they violate the policy.[1][2]

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

The Tamaqua Area School District reserves the right to determine which network services

will be provided through school district resources. It reserves the right to view and monitor all applications provided through the network and to log network use by students and staff.

E-mail is restricted to teacher-assigned projects as an integral part of a curriculum process; therefore, it is subject to review by school personnel and should never be considered private. If there is a reason to believe that e-mail is being used for purposes specifically prohibited by this policy or for illegal activity, the user account will be disabled until school authorities can confer with the user to determine the nature of the problem.

The school district reserves the right to revoke user privileges, remove user accounts, and refer matters to legal authorities when violation of this and any other applicable district policies occur, including, but not limited to, those governing network use, copyright, security, and vandalism of district resources and equipment. The Tamaqua Area School District bears no responsibility for information that is lost, damaged, or unavailable due to any cause.

Delegation of Responsibility

The district shall make every effort to ensure that these resources are used responsibly by students and staff.

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate 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 and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

The building administrators shall have the authority to determine what is appropriate use.

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 procedure shall include, but not be limited to:[1][2][3]

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.

Guidelines

Procedures

Network accounts or access to the Internet will be used only by the authorized user for its authorized purpose. Accounts/Access will be available according to a schedule developed by appropriate district authorities, given the capability of district hardware. Accounts/Access will be given out to only those individuals who meet the following requirement: have read the district's Internet policy and indicate their agreement with its provisions by signing the signature page and returning it to the appropriate district authority. Students must have their parent/guardian sign this signature page indicating the parent's/guardian's agreement

with the policy and their consent to allow the student to access and use the network.

Staff members, as part of their professional responsibility, are also expected to abide by the provisions of this agreement.

Prohibitions

The use of the Internet computer network for illegal, inappropriate, unacceptable, or unethical purposes by students or employees is prohibited. The activities listed below are strictly prohibited by all users of the network. The Tamaqua Area School District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the network. These policies are in effect any time school district resources are accessed in any way whether in school, or indirectly through another Internet Service Provider:

1. Allowing an unauthorized person to use an assigned account.
2. Use of the network for nonwork or nonschool related purposes.
3. Use of the network to access or transmit material likely to be offensive or objectionable to recipients.
4. Use of the network to communicate through e-mail for noneducational purposes or activities.
5. Use of the network to participate in inappropriate and/or objectionable discussions or news groups.
6. Use of the network to transmit hate mail, harassment, discriminatory remarks, and other antisocial communications.
7. Use of the network to order or purchase in the name of the school district or in the name of any individual any type of merchandise or service. All costs to the district or any individual incurred because of this type of violation will be the responsibility of the user.
8. Use of the network to access any fee-based online/Internet service. All costs incurred to the district or any individual because of this type of violation will be the responsibility of the user.
9. Use of the network that results in any copyright violation.[4]
10. The illegal installation, distribution, reproduction or use of copyrighted software on district computers.
11. Use of the network to intentionally obtain or modify files, passwords, or data belonging to other users.
12. Use of school technology or the network for fraudulent copying, communications or modification of materials in violation of local, state and federal laws.
13. Loading, downloading, or use of unauthorized games, programs, files or other electronic media.
14. Malicious use of the network to develop programs that harass other users or infiltrate a computer system and/or damage the software components of a computer system.

15. Destruction of district computer hardware or software.
16. Destruction, modification, abuse or unauthorized access to network hardware, software and data.
17. Acquiring or attempting to acquire passwords of others or giving your passwords to others.
18. Forging the identity of a sender or source of communication.
19. Impersonation of another user, anonymity, and pseudonyms.
20. Use of the network to facilitate any illegal activity.
21. Use of the network to misrepresent others using the network.
22. Use of the network for commercial or for-profit purposes.
23. Product advertisement or political lobbying.
24. Bullying/Cyberbullying.[5][6]
25. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
26. Unauthorized or illegal installations, distribution, reproduction, or use of copyrighted materials.
27. Access to materials, images or photographs that are obscene, pornographic, lewd or otherwise illegal.[7]
28. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
29. Inappropriate language or profanity.
30. Transmission of material likely to be offensive or objectionable to recipients.
31. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
32. Fraudulent copying, communications, or modification of materials in violations of copyright laws.[4]
33. Disruption of the work of other users.
34. Quoting of personal communications in a public forum without the original author's prior consent.

Safety

Internet safety measures shall effectively address the following:[2][3]

1. Control of access by minors to inappropriate matter on the Internet.
2. Safety and security of minors when using e-mail, chat-rooms and other forms of

direct electronic communications for educational purposes.

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 harmful materials.

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 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.

4. Report abuse to building supervisor or technical staff.

Consequences of Abuse of Responsibilities and Privileges

Any user of the network, whether student or employee, who violates the prohibitions listed in the above section of this policy, engages in any other act determined to be an unacceptable use of the network by school authorities, or violates any district policy will have his/her user privileges revoked and may be subject to other disciplinary procedures according to existing and applicable school district policies.[8][9][10][11][12]

In addition, illegal use of the network, intentional deletion or damage to files of data, destruction of hardware, copyright violations, or any other activity involving the violation of local, state, or federal laws will be reported to the appropriate legal authorities for prosecution.

Legal

1. 20 U.S.C. 6777
2. 47 U.S.C. 254
3. 47 CFR 54.520
4. Pol. 814
5. 24 P.S. 1303.1-A
6. Pol. 249
7. Pol. 237
8. Pol. 218
9. Pol. 233
10. Pol. 517
11. Pol. 317
12. Pol. 417

18 Pa. C.S.A. 2709
18 Pa. C.S.A. 5903
18 Pa. C.S.A. 6312
24 P.S. 4601 et seq
17 U.S.C. 101 et seq
18 U.S.C. 2256
20 U.S.C. 6777
Pol. 103
Pol. 104
Pol. 218.2
Pol. 220

815 Attach.doc (36 KB) 815 Consent Form.doc (27 KB)