Book	Policy Manual
Section	800 Operations
Title	Copy of Acceptable Use of Computer Networks/Digital Technology/Internet and Internet Safety
Number	815
Status	First Reading
Adopted	May 11, 1998
Last Revised	July 16, 2012
Last Reviewed	July 10, 2017

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 Titusville Area School District by providing unique resources and the opportunity for collaborative work.

Network facilities shall be used to support the district's curriculum and to support communications and research for students, teachers, administrators, and support staff.

Authority

The Titusville Area School District reserves the right to monitor and log network use and fileserver space utilization by district users. It is often necessary to access user accounts in order to perform routine maintenance and security tasks. User accounts are therefore the property of the school district. The students and staff should have no expectation of privacy or confidentiality in the content of electronic communications, Internet access, or other computer files sent and received on the school computer network or stored in his/her directory. The school computer network's system operator, or other authorized school employee, may, at any time, review the subject, content, and appropriateness of electronic communications, Internet access or other computer files and remove them if warranted, reporting any violation of rules to the school administration or law enforcement officials. The district reserves the right to remove a user account from the network to prevent further unauthorized or illegal activity if this activity is discovered.

The district recognizes the importance of teaching acceptable use and online safety to students. The district curriculum shall include instruction for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.[1][2][3]

Definitions

The **Titusville Area School District computer network** includes all local area networking and wide area networking within the school community as well as all online and direct-wired networking such as Internet to which the school network may be linked.

Digital technology shall mean all forms of digital technology, including software, hardware, and digital services of any nature and kind, that is based on digital technology that is:

1. Owned, leased, or licensed to the school district.

2. Provided directly or indirectly by the school district to its employees or students.

3. Accessed by or through digital technology that is owned, leased, or licensed to the school district.

Digital technology includes computers; servers; networks; programs; software; digital files, folders, data and records of any nature; the Internet; cell phones; beepers, PDAs; modems; voicemail; email; wikis; blogs; and such similar technologies.

User I.D. shall mean the identification number(s) or letter(s) that is unique and that is assigned to the individual student or employee.

Guidelines

Users of computer networks and other digital technology have certain privileges, rights, and responsibilities. General guidelines for use are provided within this policy, and specific guidelines for use are provided within the user agreement which shall be signed by all students and staff members who use the network. In general, these require efficient, ethical, and legal utilization of the network resources. The use of network resources, including the Internet, is a privilege, not a right, and inappropriate use shall result in a cancelation of those privileges.

The district understands the importance of teachers and students engaging, collaborating, learning, and sharing in digital environments. Students are required to demonstrate proficiency in several Pennsylvania Academic Standards for Science and Technology that relate to digital literacy skills and the use of current technology tools to design and apply advanced multimedia techniques. The district has developed the Titusville Area School District Guidelines for Using Web 2.0 Online Collaborative Media Tools to provide direction for teachers, students, and the school district community when using online media tools such as wikis, blogs, **glogs**, podcasts, video conferencing, or other online interactive media tools commonly referred to as Web 2.0 applications. Online media tools should be used only to support the curriculum and enhance teaching and learning. By accessing, creating, or contributing to any blogs, wikis, **glogs**, podcasts, or other media for classroom or district use, teachers and students agree to abide by the district's acceptable use policies and these guidelines.

The school district is not, through digital technology that is being made available to administrators, teachers, or students, creating a public forum, an open public forum, or a limited public forum. Digital technology may not be used by administrators, teachers, or students for speech or expressive conduct:[4]

1. That materially and substantially interferes with the education process.

2. That threatens immediate harm to the welfare of the school community, or to any individual(s).

3. That is lewd, vulgar, indecent or obscene or which contains sexual innuendo, metaphor or simile.

4. That encourages unlawful activity.

5. That interferes with another individual's rights.

6. That constitutes liable, slander, or defamation.

7. That is sexually, racially, or ethnically related; that is offensive, threatening, or an affront to the sensibilities of others; and that is unlawful under the standards of the antidiscrimination laws of the United States.

All expressive conduct or material (whether verbal, written, or graphic) created; downloaded; maintained; copied; pasted; harvested; or otherwise obtained; used; or transmitted by, to, from, or with the district's digital technology is required to be related to the adopted curriculum, assigned classroom activities, or school programs, such as the development of writing skills, the learning of legal, moral, and ethical restrictions imposed upon speech and the acceptance of criticism. Consequently, all expressive conduct by administrators, teachers, or students shall be:

1. Age appropriate.

2. Consistent with the rules of grammar, spelling, sentence structure, and format being taught by the district.

3. Consistent with the abilities of the student.

Communication by employees reflects on the school district. Consequently, expressive activity through digital technology shall exhibit good grammar, proper style, and good spelling. Any and all emails by an employee to any parent/guardian or student that is sent by the employee in his/her capacity as a school district employee shall be sent on and through the email account assigned by the school district. Employees are prohibited from using personal email accounts for school district business.

Employees and approved volunteers may not represent that they are communicating the views of the Titusville Area School District unless authorized by administration. Employees and approved volunteers may not act in any manner which creates the false impression that they are communicating on behalf of or as a representative of the Titusville Area School District.

Employees and approved volunteers must abide by the established school district policies regarding confidentiality and record release information of any kind when using any digital technology. This applies even if the organization, Board of School Directors, students, parents/guardians, and all current and former employees are not identified by name, but the disclosed information may enable someone to identify the individual.

This policy applies to employees and approved volunteers using digital technology while at work within the Titusville Area School District and while using digital technology when away from work. This policy does not apply to content that is unrelated to the Titusville Area School District, its Board of School Directors, students, parents/guardians, vendors, and all current and former employees.

Employees and approved volunteers are not permitted to use the Titusville Area School District letterhead in any internet posting unless authorized by the administration.

Employees and approved volunteers are personally responsible for what they post.

Employees and approved volunteers may not establish a Titusville Area School District social media site without permission.

Use of Personal Electronic Devices

The Board adopts this policy in order to maintain an educational environment that is safe and secure for district students and employees.

Violations of this policy by a student shall result in disciplinary action and may result in confiscation of the electronic device. The confiscated item may not be returned until a conference has been held with a parent/guardian.

Mobile Devices

The policy and guidelines in this section apply in its entirety to students in grades 9-12 only. For students in grades K4 -8 mobile devices can be used with the exception of cell phones. Cell phones are not permitted to be used by these students during school hours. Cell phones must remain in their lockers or backpacks and are to be shut off. Other mobile devices such as personal digital e-readers, tablets and laptops may be used in school for instructional purposes only.

Mobile devices are powerful communication tools. They have the ability to not only enable voice-to-voice conversations, but they allow us to communicate via text messaging, email, and on many devices via the world-wide web. To completely ban mobile devices from the classroom is to cut students off from the very world for which we are preparing them. However, for the very same reasons mobile devices can be considered a classroom distraction. Therefore, the following guidelines have been created to support educators that choose to empower students to use their devices for instructional purposes:

1. Have an instructional objective. Using technology in the classroom is typically very engaging for students. However, technology should be more than just engaging. It should empower teachers and students to meet objectives they cannot otherwise meet.

2. Communicate with parents/guardians. Even though this language is now a part of the Student Handbook, parents/guardians may not remember signing or they may wish to change their permission selection once they know how the cell phones are being used in class. For example, most cell phones that students carry are paid for and belong to their parents/guardians. Prior to students using their cell phones as a classroom tool, teachers will notify parents/guardians in this regard.

3. Teachers may check student accounts on the public drive to see if permission for the use of mobile devices was granted by parents/guardians.

4. Rules for the use of mobile devices are made to ensure the devices are being used for instructional purposes. Devices that are being used in any other way are in violation of the district policy regarding the use of electronic devices.

5. Rules are:

    a. When using mobile devices to access the Internet, students are required to connect using the TASD network.

    b. Mobile devices need to be on vibrate.

    c. Mobile devices need to be in pockets or backpacks until it is time to use the devices.

d. Mobile devices can only be used in class for academic/learning purposes.

e. Any activity conducted on mobile devices in class cannot be published without permission of teacher and/or students who are involved in the text/image/video/audio file (e.g. no publishing a photo of a class project on any social networking site without permission).

f. Students will use appropriate mobile device etiquette by respecting the privacy of other's device numbers and using appropriate language with their mobile communication.

Acceptable Use

The use of the computer network and other digital technology must be in support of education and research and consistent with the educational objectives of the Titusville Area 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. Use of any district computer or other digital technology, unless and until the individual has signed an acknowledgement in the form prescribed by the district attesting to the individual's understanding of the rules governing acceptable use of computers and other digital technology, is prohibited.

Students are required to submit an acceptable use agreement signed by the student and a parent/guardian at the beginning of each school year. As long as the student remains in the same school building, the acceptable use agreement shall remain in effect until September 30 of the following year to provide ample time for students to return a new signed agreement. Any student who moves from one building to another at the end of the school year must submit a signed agreement prior to being allowed to use the district's computer network.

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

The use of the computer network for illegal, inappropriate, or unethical purposes by students or employees is prohibited. More specifically, the following uses are prohibited:

1. Use of the network to facilitate illegal activity.

2. Use of the network for commercial or for-profit purposes.

3. Use of the network for nonwork or nonschool related work.

4. Use of the network for product advertisement or political lobbying.

5. Use of the network for hate mail, discriminatory remarks, and offensive or inflammatory communication.

6. Unauthorized use of network facilities or digital technology for fraudulent reproduction, installation, distribution, communications, or modification of materials in violation of copyright laws.

7. Use of the network to access obscene, sexually explicit or pornographic material, or failure to report (to a teacher for students and to the network administrator for district employees) any time when s/he inadvertently visits or accesses a pornographic site.[3]

8. Use of inappropriate language or profanity on the network.

9. Use of the network to transmit material likely to be offensive or objectionable to recipients.

10. Use of the network to intentionally, "hack" into anyone else's computer and willfully, maliciously, or through reckless indifference obtain or modify files, passwords, and data belonging to other users.[5]

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

12. Loading or use of unauthorized games, screensavers, programs, files, or other electronic media.

13. Use of the network to disrupt the work of other users.

14. Destruction, modification, or abuse of network hardware and software.

15. Quoting personal communications in a public forum without the original author's prior consent.

16. Use of any district computer unless and until a confidential user I.D. and password has been assigned to the student or employee.

17. Use of any district computer without using his/her user I.D. and password.

18. Terminating use of any district computer without logging off the computer.

19. Attempting to bypass any blocking software that may be used or installed by the district.

20. Violating the district's Code of Student Conduct or any other applicable policy of the district.

21. Intentionally entering any secure or confidential area of the district's systems, network(s), computers or other digital technology without proper authority.

22. Violating the legal rights of others.

23. Knowingly infecting or planting any virus, pornography, or other prohibited content or software on anyone's computer or other digital technology.

24. Use of any software or Internet site in violation of any applicable licensing agreement or applicable terms of use.

25. Use of any data mining or similar data gathering and extraction methods in violation of any person's or entity's rights.

26. Use of digital technology to violate any applicable law, including the Wiretap and Electronic Surveillance Control Act.

27. Deleting or removing any program, application, security feature, or virus protection from any district computer or other digital technology.

28. Violating any applicable criminal statute pertaining to computers, property, or electronic devices, including Chapter 76 of the Crimes Code, relating to computer offenses (18 Pa. C.S.A. §7601 et seq).[6]

Security

System security is protected through the use of user I.D.'s and 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. Employees or students shall not use or utilize the user I.D. and/or password belonging to or assigned to any other individual, or impersonate, in any manner, any other person. Users are not to use a computer that has been logged in under another student's or teacher'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.

Password Policy

Students will be assigned a password protected account for access to the computer network and internet. However, all passwords will be static and will remain the same throughout the school year unless a breech in security warrants the network administrator to change the password.

Safety and Protection of Personal Information

When sending electronic messages, students and staff shall not include personal information, such as addresses and phone numbers that could identify themselves or other students and staff. Internet I.D. and passwords are provided only for personal use. Students and staff shall not share their password with anyone and shall not use anyone else's password, regardless of how the password was obtained. Those who suspect that someone has discovered their password shall change it immediately. Students and staff shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.

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

1. Any network user who receives threatening or unwelcome communications shall immediately

bring these to the attention of a teacher or administrator.

2. Network users shall not reveal personal addresses or telephone numbers to other users on the network.

Copyright Infringement

Students and staff shall not:

1. Copy and forward.

2. Copy and download.

3. Copy and upload to the network or Internet server any copyrighted material without approval by the computer system operator, a teacher, or other school administrator. **Copyrighted material** is anything written by someone else including but not limited to a game, a story, an encyclopedia entry, or software.[5][7]

Commercial Use

Students and staff shall not use the school district's computer network to solicit sales or conduct business (e.g., by posting an advertisement to a news group or by setting up web pages to advertise or sell a service without the approval of the Board of School Directors).

Consequences for Inappropriate Use

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

2. Failure to follow the procedures and prohibited uses previously listed in this policy may result in loss of network access. Other appropriate disciplinary action may also follow.

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

4. Violations of this policy by an employee or student may result in corrective action up to and including:

    a. Suspension or termination of employment for employees.

    b. Suspension or expulsion for students

Google Apps for Education

Google Apps for Education is a service from Google that provides independently customizable versions of several Google products enabled by Titusville Area School District. It features several applications with similar functionality to traditional office suites, including Gmail, Google Calendar, Drive, Docs, sheets and Slides. All work is stored in the cloud and is accessible from any internet connected computer by using the account provided by Titusville Area School District.

Legal

1. 24 P.S. 1303.1-A
2. 24 P.S. 4601 et seq
3. 47 U.S.C. 254
4. Pol. 220
5. Pol. 814
6. 18 Pa. C.S.A. 7601 et seq
7. 17 U.S.C. 101 et seq

18 Pa. C.S.A. 5903

18 Pa. C.S.A. 6312

18 U.S.C. 2256

20 U.S.C. 6777

47 CFR 54.520

Pol. 103

Pol. 103.1

Pol. 104

Pol. 218

Pol. 218.2

Pol. 233

Pol. 237

Pol. 248

Pol. 249

Pol. 317

Pol. 348

815 Chromebook Acceptable Use Policy Admin Guidelines.pdf (92 KB)

815 iPad Acceptable Use Policy Administrative Guidelines.pdf (329 KB)

Last Modified by Jane McNierney on August 4, 2017