Book	Policy Manual
Section	800 Operations
Title	Utilization of Technology
Code	815
Status	Active
Adopted	November 21, 2013
Last Revised	September 25, 2017
Last Reviewed	August 17, 2017

Purpose

Philosophy

The district's technology is an integral part of the instructional program and serves as a support system for district operations.

The protection of district interests, the technology itself, and most of all the users, both students and staff, is crucial.

Purpose of Use

Primary uses of district technology shall be as follows:

1. For curriculum-based instruction of students.
2. School-related activities.
3. Staff development.
4. Adult education.
5. For the administrative operations of the district.

Students may make other appropriate and responsible use of technology only with the authorization of a district staff member.

Authority

The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.

The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized illegal use will result in cancelation of those privileges and appropriate disciplinary action.

The district recognizes the importance of teaching acceptable use and online safety to students. The district shall educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and in cyberbullying awareness and response.

Delegation of Responsibility

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 administrator shall have the authority to determine what is and is not inappropriate 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 procedures shall include but not be limited to:[1][2]

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.[3]
2. Monitoring online activities of minors.

The district shall provide a copy of this policy to parents/guardians, upon written request.[3]

Guidelines

Access to the System

Network user accounts will be used only by the authorized owner of the account for its authorized purpose.

Accounts will be provided only to those individuals who have successfully completed a learning experience, which will include, but not be limited to, instruction on network access, use, acceptable vs. unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities. This requirement shall apply to both students and district employees.

Operations

Employees and students shall be responsible for reading and understanding the contents of this policy.

Faculty assigned to teach in classrooms which incorporate technology shall inform students of their responsibilities and the penalties that shall be imposed for misuse of technology.

Where district time and/or technologies are utilized by staff members to create resources, the product will be considered under the guidelines of work for hire and will become the property of the district.

Employees and students shall be responsible for adhering to this policy and to all operational guidelines related to technology.

The district maintains the right to assign penalties or charge fair market value for equipment damaged or destroyed by accident or through negligence when the equipment is under the care or assigned to an individual.

No user of district technology resources should expect that any files, documents, or communications are private.

The district reserves the right to monitor and copy any product created or accessed by utilizing district technology resources.

All users must be responsible for keeping passwords secured and confidential.

Students who inadvertently access a restricted site are responsible to bring such action to the immediate attention of their instructor/advisor.

Employees who inadvertently access a restricted site are responsible to immediately exit the site and report these facts to their immediate supervisor.

Individuals are encouraged to report inappropriate or irresponsible uses of technology to the building principal or to the Superintendent.

Incidental Personal Use

Use by an individual employee for occasional personal communications. Personal use must comply with this policy and all other policies, procedures and rules, and may not interfere with the employee's job duties and performance, with the system operations, or with other system users. Under no circumstances should the employee believe their use is private, the district reserves the right to monitor access and use of its network.

Restricted Use/Prohibited Activities

In accordance with district policy, accepted rules of network etiquette, and federal and state law, the following uses of technologies are prohibited:

1. Use of technology for defamatory, abusive, obscene, profane, sexually oriented, threatening, offensive and/or illegal materials.
2. Use of technology for commercial gain or profit.
3. Transferring copyrighted materials to or from any district technology equipment without the express consent of the owner of the copyright.
4. Bullying/Cyberbullying.[4][5]
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Access to obscene or pornographic material or child pornography.
7. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
8. Impersonation of another user, anonymity, and pseudonyms.
9. Loading or using of unauthorized games, programs, files, or other electronic media.
10. Disruption of the work of other users.

Staff or students illegally accessing, altering, damaging, or destroying any technology equipment, computer network, computer software, or system information within a school system or an external system will be referred to the Pottstown Police Department for investigation and possible prosecution.

Access and Security Prohibitions

Users must immediately notify the Director of Technology if they have identified a possible security problem. The following activities related to access to the district's computer network and the Internet are prohibited:

1. Misrepresentation, including forgery, of the identity of a sender or source of communication.
2. Acquiring or attempting to acquire passwords of others or giving your password to another.
3. Revealing a password or otherwise permitting the use of others, by intent or negligence, of personal accounts for computer and network access.
4. Using or attempting to use computer accounts of others; these actions are illegal, even if only for the purposes of "browsing".
5. Altering communication originally received from another person or computer with the intent to deceive.
6. Use of the district system to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, or being involved in a terroristic threat against any person or property.
7. Disabling virus protection software or procedures.

Such violations in the case of students may result in suspension and/or expulsion, and such violations on the part of employees will constitute just cause for dismissal.

Sharing individually assigned accounts and passwords is prohibited. Passwords are designed to protect and any attempt to circumvent system security to gain unauthorized access to technology resources is expressly prohibited and subject to the appropriate punishment.

Student and staff photographs and names that are made available in district-sponsored media are permitted to be displayed on the district website.

Student and staff photographs and names may be displayed on other commercial sites with specific written approval of the Superintendent and parents/guardians.

Students shall not download any information from the Wide Area Network/Internet unrelated to their specific course of study without prior approval of their instructor.

Any commercial endorsement placed on or linked to the district website shall require the written approval of the Superintendent.

Users will not use the district system for political lobbying.

Actions Resulting From Misuse

Inappropriate or irresponsible use of technology will result in the following actions:

1. In cases where a law or copyright has been violated, a referral shall be made to appropriate law enforcement officials. Such violations in the case of students may result in suspension and/or expulsion, and such violations of the part of employees will constitute just cause for dismissal.
2. Student infractions which are not deemed illegal will result in appropriate school discipline being imposed and/or reviewed by the building principal.
3. Employee infractions which are not deemed illegal but violate Board policy will result in appropriate administrative action/discipline, which may include termination of employment.
4. The user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.
5. Vandalism will result in cancelation of access privileges. 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.

Copyright

Staff members shall not violate any contractual limitations concerning the use of software. Software shall not be copied or transferred without the expressed permission of the district's Technology Director.

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.[6]

Internet Access

Internet access shall be governed by the same rules and regulations set forth in this policy relating to the utilization of technology.

Elementary School Students – No elementary student will access the Internet directly on his/her own. Internet access at the elementary level will be limited to teacher-directed and teacher-demonstrated use.

Middle School And High School Students – Starting in 5th grade, students may have the opportunity to access Internet services at the direction of a staff member. Internet access is a privilege, not a right, and may be removed if any portion of this policy is violated or if the privilege is abused in any other way. Students in the middle school will not access the Internet without direct supervision by an adult, such as a teacher or other staff member (e.g., classroom aide).

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications 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, Internet, etc.

Users will not post personal contact information about themselves or other people. In other words, the user may not steal another's identity in any way, may not use spyware, cookies, or use the network in any way to invade privacy. Additionally, the user may not disclose, use or disseminate personal information of other students or employees including, but not limited to, student's grades, Social Security numbers, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, and educational records. Personal contact information includes home address, telephone numbers, school address, and work address.

Student users will agree not to meet with someone they have met online.

Documents or videotapes may not include information which indicates the physical location of a student at a given time other than attendance at a particular school or participation in school activities, unless authorized by administration.

Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software, unless otherwise approved by the superintendent of schools.[1][2]

Internet safety measures shall effectively address the following:[1]

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.

Email Accounts

Email Accounts for Students: Elementary students will not be provided with email accounts with limited exceptions. Students may have email access through a classroom account. Students may be approved to use an email account for limited educational purposes. At the high school level, students are given an individual district email account.

Email Accounts for District Employees and Board Members: District employees and Board members may be provided with an individual account.

Executive Secretary Access to Email Account: It will not be considered a violation of this policy if and when an executive secretary is called upon to access and use the email accounts, calendar accounts, or other system software accounts of the executive administrator to whom he/she reports when authorized to do so.

Guest Accounts: Guests may receive an individual account with the approval of a district administrator if there is a specific, district-related purpose requiring such access. Use of the system by a guest must be specifically limited to the district-related purpose. A signed agreement is required and the signature of a parent/guardian will be required if the guest is a minor.

Establishment of Websites

The district may establish a website and develop web pages that present information about the district.

A district-appointed employee or third party, under the supervision and direction of the Director of Community Relations, will be responsible for maintaining the district website.

Websites under the heading or affiliated with the district will be considered as district publications and will be subject to approval by a district representative authorized by the Superintendent.

Personal Web Pages: District employees, Board members or guests may not establish personal web pages using district resources.

School or Class Web Pages: Schools, classes, and staff may establish web pages that present information about the school or class activities.

Students may not establish personal websites with any link or affiliation with the district.

Parental Notification and Responsibility

The district will notify the parent/guardian about the district system and the policies governing its use.

The district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their child(ren). The district encourages parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the district system.

School Board Use of Electronic Mail

Use of electronic mail (email) by Board members should conform to the same standards of judgment, propriety and ethics as other forms of Board-related communication.

The Board shall not use email as a substitute for deliberations at Board meetings or for other communications or business properly confined to Board meetings.

Board members should be aware that email and email attachments received or prepared for use in Board business or containing information relating to Board business may be regarded as public records which may be inspected by any person upon request, unless made confidential by law.[7]

Board members should avoid reference to confidential information about employees, students or other matters in email communications because of the risk of improper disclosure. Board members should comply with the same standards as school employees with regard to confidential information.

District Limitation of Liability

The district make no warranties of any kind, either express or implied, that the functions or the services provided by or through the district system are error-free or without defect. The district will not be responsible for any damage users may suffer, including but not limited to loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.

District personnel shall not be responsible for monitoring student use of the Internet or email when students are accessing the system from home.

Legal

1. 47 U.S.C. 254
2. 20 U.S.C. 6777
3. 24 P.S. 4604
4. 24 P.S. 1303.1-A
5. Pol. 249
6. Pol. 814
7. Pol. 801

17 U.S.C. 101 et seq
18 Pa. C.S.A. 5903
18 Pa. C.S.A. 6312
18 U.S.C. 2256
24 P.S. 4601 et seq
47 CFR 54.520
Pol. 103
Pol. 104
Pol. 218
Pol. 218.2
Pol. 233
Pol. 248
Pol. 317
Pol. 348