BRADFORD AREA SCHOOL DISTRICT

TECHNOLOGY AND COMPUTERS

ADOPTED: May 19, 1997

REVISED: April 10, 2000
November 11, 2002
September 15, 2008

	814.1. ACCEPTABLE USE OF TECHNOLOGY AND COMPUTERS
1. Purpose	The purpose of this policy is to outline the acceptable uses of technology, including but not limited to hardware devices, software, network and Internet access in the Bradford Area School District and to define the consequences of misuse. For the purpose of this document, a **user** is defined as an administrator, teacher, student, community member, invited guest, or other individuals employed by the Bradford Area School District. All technology, to include computers, in the Bradford Area School District have been purchased and installed for instructional and administrative use only. The software installed on each computer and network has been purchased by the district and licensed for use herein. Because the computers are used in a variety of classroom situations, it is critical that each workstation operates as it was meant to in each instance.
2. Authority	The Board establishes that the use of technology in the Bradford Area School District is a privilege, not a right; inappropriate, unauthorized and illegal use can result in the cancellation of those privileges and the application of appropriate disciplinary action.
3. Guidelines	All users must read, sign and return the appropriate acceptable use acknowledgement form before being granted access to district technology. Students will sign as well as obtain their parent/guardian signature and return the appropriate form to their teachers. Student forms will be maintained by the building librarian. All staff and other user forms will be returned to and maintained by the technology department. It is the policy of the district not to allow games to be installed or played on the computers unless specifically permitted by the teacher. In those instances, only games installed by the district technology staff shall be permitted. Students playing games without the express consent of the teacher may be disciplined, lose their computer privileges for a set period of time or may face loss of credit for the current assignment.

All computer and technology updates will be performed by the technology staff only. Inventory of technology assets is critical to equipment management and accountability. All district-owned computers and technology resources will not be removed from district property unless prior written consent by the district's designated technology administrator is granted. Additionally, all computers and technology devices will remain in their assigned rooms and only moved by technology staff upon request and approval.

Portable and/or mobile technology devices and equipment such as mobile laptop carts, cameras, etc. may be moved within the assigned areas of the building. All portable and mobile technology equipment will have a chain of custody procedure to maintain equipment accountability. All users will complete the custody procedures when receiving and returning the equipment or devices.

Intentionally altering the installed software or hardware settings of the district's computers and other technology resources disrupts the learning process for both staff and students. Staff and students may not misuse or alter the district's technology and computers in any way, including but not limited to the following:

1. Installing, altering or deleting district, personal, share-ware or copyrighted software.

2. Removing, changing or damaging any hardware or settings on said computers or on installed software.

3. Using the computers in any malicious manner (including harassment, cyber bullying, discrimination, hate mail or other antisocial behavior).

4. Accessing, processing or transmitting arguably pornographic or sexually explicit materials, inappropriate text files, copyrighted materials or any other files which may be dangerous to the maintenance of the integrity of the district's computer systems.

5. Seeking information, obtaining copies or modifying files, data or passwords which belong to others.

6. Using the district's computers for personal, business or financial gain.

7. Using the district's computers/networks other than for authorized and educational purposes inappropriately while working at a workstation or logged into the Internet.

8. Introducing any virus program into the district's workstations or networks.

	9. Using the workstations or network to facilitate hacking and other illegal activities such as pirating of music, movies or software. 10. Using the workstations or network for product endorsement or advertisement or for political activities. 11. Loading or use of unauthorized games, programs, files or other electronic media. 12. Impersonation of another user or the use of anonymity and pseudonyms. 13. Quoting personal communications in a public forum without the original authors' prior written consent.
20 U.S.C. Sec. 1232g 34 CFR Part 99	14. Transmission of any personnel or student information, which is protected by the Family Educational Rights and Privacy Act.
Pol. 218	Student disciplinary action for these and any other acts of misconduct will be dealt with in accordance with this policy and the district's student conduct code. Such discipline may include any, or all, of the following: 1. Removal of the student from the course for some set period of time. 2. Detention and/or in-school suspension from school. 3. Out-of-school suspension from school. 4. Expulsion from school. 5. Reimbursement for damaged equipment or software. 6. Reimbursement for repair time for damaged equipment and software at the in-house rate of $60/hour or the contracted hourly service provider's rate and for the replacement of said hardware or software, whichever is applicable. 7. Completion of a mandated training session prior to being allowed to resume access to the district's technology hardware and/or software. 8. Banishment from using the respective technology hardware and/or software. 9. Subject to criminal prosecution under state and federal laws.

Each user will be held responsible for any intentional alteration of a computer workstation that occurs while s/he is working at that station, or while such station has been signed over to the user. Where a student is receiving Learning Support Services the applicable state guidelines will be followed. Each user must report any damages or errors encountered to the respective classroom teacher, supervisor, administrator, and technology staff as soon as discovered. Staff and students are reminded that the district's computers are provided primarily for instructional use; student use takes priority over staff use.

In addition to user responsibilities, each teacher and staff member will be responsible for monitoring, supervising and enforcing this policy for each user under their supervision. Infractions will be acted upon and reported to their respective supervisor in a timely manner. All infractions will be reported to the district's technology administrator.

Misuse or misconduct by staff members will be consistent with law and handled in accordance with employment policies and procedures.

Network, Online And Internet Access

The Board supports the use of the Internet and other computer networks in the district's instructional program to facilitate learning and teaching through interpersonal communications, access to information research and collaboration. The use of all network facilities shall be conducted within the framework and authority of the district policies, procedures, and the federal and state Children's Internet Protection Acts. Additionally, it shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities and developmental levels of the students.

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of students and relevant to course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of material contained on or accessed through the web site.

Web-based services such as Blackboard, moodle, wiki, blogs and other collaboration tools that emphasize online educational collaboration and sharing among users may be permitted; however, the district technology administrator must approve such use. Users must comply with this policy as well as other relevant policy, regulations, and procedures.

Use of the district's hardware shall not imply endorsement of the content of any electronic information so used, nor does the district guarantee the accuracy of any information received through such networking services. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network, online service or the Internet.

The district shall not be responsible for any unauthorized fees or charges resulting from access to the online services or the Internet. It also reserves the right to log network use and to monitor fileserver space utilization by users, while protecting the rights of such users. Students and staff have the responsibility to respect and protect those rights in the district and on the Internet. The district shall make every effort to ensure that this educational resource is used responsibly by students and staff.

The district's technology administrator shall have the final authority to determine what is inappropriate use.

Active Restriction Measures

20 U.S.C. Sec. 6777
47 U.S.C. Sec. 254

The district will utilize filtering software or other technologies to prevent users from accessing material and visual depictions that are: (1) obscene, (2) pornography, or (3) harmful to minors. The district will monitor the online activities of all users, through direct observation and/or technological means, to ensure that users are not accessing such depictions or other material that is inappropriate.

Internet filtering may be disabled by the district's designated technology administrator as necessary for the purpose of valid research or other instructional projects being conducted by a user(s).

18 Pa. C.S.A. Sec. 5903

The term **harmful to minors** is defined as meaning the quality of any description or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when:

1. It predominantly appeals to prurient, shameful, or morbid interest of minors.

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

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

Network Accounts

Network accounts will be used only by the authorized owner of the account and only for its authorized purpose. All communications and information accessible via the network should be assumed to be the property of the user, subject to review by district's staff, as may be needed, and shall not be disclosed to other users. Network users shall respect the privacy of others on the system.

Network Prohibitions

Students and staff 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. Examples of non-acceptable behavior are included herein:

1. No personal or non-district owned computers or devices will be connected to the district network or Internet, including wireless devices.

2. No spoofing of MAC or IP addresses to gain access to district network or Internet.

3. The use of proxy servers or other means to bypass Internet filtering and network security is prohibited.

4. No programs, plug-ins or executable (.exe) software will be stored in shared network folders and home directories (personal folders).

Security

System security is protected through the use of software and passwords. Failure to adequately protect and 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. Staff (except to system administrators) and students (except to staff and system administrators) shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged into under another user'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 district's workstations and/or to the network.

	The district provides e-mail services to staff members only for work-related use as needed, not for personal use or union matters, unless written pre-approval is granted by the Director of Human Resources. When granted, use will be restricted only to union officials. The same acceptable use policies listed for computer use also apply to e-mail services. The district may monitor e-mail messages sent or received through the district's Wide Area Network. Users of the network must realize that the district has this authority to intercept e-mail messages and that there will be no privacy rights construed by the district to exist covering any statements or messages made in or through the network. No personal online e-mail may be accessed while using the district's Wide Area Network. The district's administration reserves the right to monitor and access all accounts on the system. Professional staff of the district will monitor the use of the Internet by their respective students. <u>Safety</u> To the greatest extent possible, users of the district's computers and technology hardware shall be protected from harassment or unwanted or unsolicited communication. Any user who receives threatening or unwelcome communications shall immediately notify his/her teacher or administrator. <u>Consequences</u> Both network and other users shall be responsible for damages to the equipment, systems and software resulting from deliberate or willful acts. Misuses of the district's equipment and software is defined elsewhere in this policy. <u>Copyright</u>
Pol. 814	The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from a network, online service or the Internet shall be subject to fair use guidelines. This includes pirating of music, movies or other downloadable files and media. <u>District Web Sites</u> The district will establish a web site and will develop web pages that will present information about the school district. The district's technology administrator, or his/her designee, will be designated as the district webmaster and will be responsible for maintaining district web sites. Only the webmaster shall be authorized to access district web sites for the purpose of amending, adding, or deleting information.

	Information posted on district web pages shall be kept current; those not so maintained may be amended or deleted at the direction of the webmaster. School Or Class Web Sites Schools and classes may establish web pages that present information about the school or class activities. All information shall be reviewed and approved by both the building principal, or his/her designee, and the district's webmaster. Organizational Web Pages With the approval of the building principal, or his/her designee, and webmaster, school-related organizations and athletic groups may establish web pages for specifically defined activities. The principal and webmaster shall establish criteria for the establishment of such pages and for the posting of material on these pages. Materials presented by the organization must relate specifically to organizational activities and must contain only student-produced information and supporting materials. All information shall be reviewed and approved by both the principal, or his/her designee, and the district's webmaster. District Web Site Use Students will not post personal contact information about themselves or other people, including links to any personal web pages. **Personal contact information** includes, but is not limited to, home address, home telephone, school address, school telephone, work address, personal web site, etc. Teachers, principals and the district's webmaster will ensure that student names will not be made available on either the district's Intranet or on the Internet. Student pictures may only be used with the signed consent of the parent(s)/guardian(s) or with the consent of a student eighteen (18) years of age or over. Such consent may be given on the respective annual technology use form. Additionally, the use of any student picture must be directly related to district educational, athletic, or extracurricular activity, and the photograph must focus primarily on the activity or the resulting product of that activity.
Pol. 218	Students shall not attempt to gain unauthorized access to any district-authorized web site. Unauthorized activity will subject the student to disciplinary actions as set forth in the district's code of student conduct.

References:

Crimes and Offenses, Definition of Specific Offenses – 18 Pa. C.S.A. Sec. 5903, 6312

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

Family Educational Rights and Privacy Act – 20 U.S.C. Sec. 1232g

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

Family Educational Rights and Privacy, Title 34, Code of Federal Regulations – 34 CFR Part 99

Board Policy – 218, 237, 814