SCHOOL DISTRICT OF PITTSVILLE

BOARD POLICY

INSTRUCTIONAL RESOURCES AND SERVICES

ACCESS/USE OF INSTRUCTIONAL TECHNOLOGY

INTERNET SAFETY AND TECHNOLOGY USE 363.2

Purpose

The Pittsville School District is providing access to a network that contains Internet access. The purpose of this policy is to set forth procedures and guidelines for access to the school district computer system, student use of technology, and safe, acceptable use of the Internet.

1. General

Computer networks, including the Internet, offer vast, diverse, and unique resources to both students and teachers. Our goal in providing these services to staff and students is to promote learning, facilitating resource sharing, innovation, and communication.

Through network access, learners will:

- utilize a personalized, motivational learning opportunity
- enter into partnerships to enhance their learning options
- gain an employability skill needed for the 21st century
- broaden their problem-solving and decision-making abilities
- broaden their research capabilities by using primary materials
- develop their higher-level thinking skills
- access global resources

With access to computers and people all over the world comes the availability of material that may not be considered to be of educational value in the context of the school setting. However, on a global network, it is impossible to control all materials and an industrious user may discover controversial information. We firmly believe that the valuable information and interaction available on a network and on the Internet far outweigh the possibility that users may produce material that is not consistent with the educational goals of the District.

2. Limited Educational Purpose

The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines as provided below. In general, this requires efficient, ethical, and legal utilization of the network resources for educational purposes only. As students/staff use this network, it is essential that each user recognize his or her responsibility in having access to the vast services, sites, and people. The user is ultimately responsible for his or her own actions in accessing network services, and for adhering to district use policies, procedures, and guidelines. If a user violates these provisions, his or her account or network access will be limited or terminated, future access could be limited or denied, and legal referrals may be made. The signatures at the end of this document are legally binding and indicate the parties who have signed have read the terms and conditions carefully and understand their significance.

All groups or individuals will be required to follow state statutes concerning computer crimes (943.70), follow educational goals of the school and work within the confines of applicable provisions of current collective bargaining agreements, and other school district policies. All groups or individuals who utilize the District's computer network acknowledge their receipt of, review of, and understanding of the School District's Student

Internet Safety and Technology Use Agreement. Any violation of the Agreement shall subject the user to the most appropriate form of discipline under this Agreement. Furthermore, the School District of Pittsville reserves the right, from time to time, to amend the rules and policies. In such event, copies of the same shall be distributed to each user who has executed this Agreement.

Before students will be allowed to use any network or computer/electronic device, or connect to the Internet or other district network resources using district owned or personal electronic devices, this Student Internet Safety and Technology Use Policy must be read and agreed to by the user and the parent or guardian, if a minor child.

3. Privileges

The network hardware and software are the property of the School District of Pittsville. The use of the network is a privilege, not a right. Inappropriate use will result in cancellation of those privileges and possible legal referral. The system administrator(s) may suspend an account or disallow access at any time for violation of these guidelines, or if a user is identified as a security risk. The administration may request the system administrator to deny, revoke, or suspend specific user accounts or access.

4. Acceptable Use

The use of an account or access to the network or Internet must be in support of education and research and consistent with the educational objectives of the Pittsville School District, including use of the system for classroom activities, professional or career development, self-discovery activities, and pursuit of educational and personal goals consistent with the mission of the school district and school policies.

Uses that might be acceptable on a private or home account or on another system may not be acceptable on this limited purpose network. Use of other organization's network or computing resources must comply with the rules appropriate for that network, including generally accepted rules of network and Internet etiquette.

5. Unacceptable Use

Unacceptable use of the computer network or Internet shall include but not be limited to the following:

(a) Use of the school district system for commercial activities, product advertisements, financial gain, or political lobbying.

(b) Use of the school district system to transmit, receive, access, review, upload, download, store, print, post, or distribute pornographic, prurient, obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language, images or other material that is lacking educational merit, socially redeeming value or that is disruptive to the educational process.

(c) Use of the school district system to access, review, upload, download, store, print, post, or distribute materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination.

(d) Use the school district system to knowingly or recklessly post false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.

(e) Any use of the school district system in such a way that would interfere with the efficient operation of the network or disrupt the use of the network by others, (e.g. downloading excessively large files or emailing excessively large documents).

(f) Unauthorized use of other email systems (such as Hotmail), chat rooms, message boards, Listservs, instant messaging or other email services, including signing up for periodical message services such as "Joke of the Day," or other services over the Internet, or the sending of unwanted or "nuisance" E-mail/chain messages (SPAM) which are not consistent with the Acceptable Use policy defined above.

(g) Attempting to access prohibited social networking sites (such as Facebook, MySpace, etc.), graphics, photo or video networking sites without permission of a staff member. Use of social networking resources must be for educational purposes and must comply with all district policies, procedures, and computer etiquette.

(h) Attempting to download, run, load, modify, or install programs or software on the network, server, or workstation/computer hard disk or other storage media (such as USB flash drives) without the permission and assistance from the system's administrator. Use of software on the network or workstation is limited to that which has been legally licensed and properly installed.

(i) Use of the school district system to download programs, music files (such as MP3), images, or other software or files for personal use or for any use not consistent with the Acceptable Use policy defined above, without prior permission.

(j) Use of school district system to download, run, load, or install games or to run, access, or play games over the Internet without permission from a staff member. The playing of games, whether locally or over the Internet must be for an educational purpose and must comply with all aspects of this Student Internet Safety and Technology Use Policy.

(k) Use of the school district system to vandalize, damage or disable the property or data of another person or organization; deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means; tampering with, modifying or attempting to harm, destroy or change the school district system software, hardware or wiring or take any action to violate the school district system's security.

(l) Attempting to log on as system administrator, or gain unauthorized access to the school district system or any other system through the school district system; attempting to log in through another person's account, or obtain passwords, use computer accounts, access codes or network identification other than those assigned to the user; attempting to discover passwords or gain access through the use of "hacker" programs or similar activities.

(m) Use of the school district system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

(n) Use of the school district system to post private information about another person or to post personal contact information about themselves or other persons (unless for official school business or otherwise authorized) including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords.

(o) Use of the school district system to violate copyright laws or usage licensing agreements, plagiarize or otherwise use another person's property without prior approval or proper citation, including the downloading or exchanging of pirated software. All users must comply with the District's Copyright Policy #361.21.

(p) Any attempt to bypass or circumvent the district's Internet filtering system as described in 9(a) below through the use of programs either downloaded from the Internet or brought in on portable storage devices (such as USB flash drives), or through other Websites or Web services such as proxies, or through any other means which results in the user's Internet access bypassing, circumventing or otherwise avoiding our Internet filter.

(q) Any other violations of accepted network or Internet etiquette.

(r) Use of the school district system to engage in or support any illegal activity or violate any local, state or federal statute or law.

6. Security

Maintaining the security and integrity of the computer network is the responsibility of all users. Users must notify the system administrator of security problems. Users should not demonstrate the problem to other users. Users should report any inappropriate use of the network to an administrator. Any user identified as a security risk or having a history of problems with other systems may be denied access to the network. Users are expected to comply with any additional restrictions or procedures determined by the system's administrator.

7. Violations

In the event a student breaches any part of this Student Internet Safety and Technology Use Policy, there will be consequences imposed by the school, consistent with the Parent/Student Handbook and District policies. Each situation will be considered independently and consequences will range from a discussion about the rules and expectations regarding technology/Internet usage and/or a complete withdrawal of access to all computer technology up to and including suspension or expulsion. Violations could also lead to referral to local police authorities.

If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to an appropriate school district official. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. A user may also in certain instances access otherwise unacceptable materials if necessary to complete an assignment and if done with the prior approval of and with appropriate guidance from the appropriate teacher.

8. Limited Expectation of Privacy

(a) By authorizing use of the school district system, the school district does not relinquish control over materials on the system or contained in files on the system. Users should expect only limited privacy in the contents of personal files on the school district system.

(b) Routine maintenance and monitoring of the school district system may lead to a discovery that a user has violated this policy, another school district policy, or the law. An investigation or search will be conducted if the school authorities have a reasonable suspicion that the search will uncover a violation of law or of school district policy.

(c) Parents have the right at any time to investigate or review the contents of their child's files and email. Parents have the right to request suspension or termination of their child's account at any time.

(d) The school district will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school system.

(e) Users must take care that they do not disclose, use, or disseminate personal information, including historical records, regarding minors or other users when using the school district system, unless authorized to do so.

9. Internet Use

(a) All networked computers in the Pittsville school district have access to the Internet through dedicated fiber optic lines. This access is filtered by software that is designed to limit access to Internet sites that may not be in compliance with district policies, harmful to minors, or are of little or no educational value. Filtering software is not perfect and does not catch all objectionable sites, and in other instances, mistakenly filters out sites that are not objectionable. Furthermore, it is not currently possible to filter all forms of electronic mail, chat rooms, instant messaging, or other forms of electronic communications. Therefore, it is the responsibility of users to ensure that such use complies with district policies. Any errors in filtering should be reported to the system administrator. Web sites, portals or other Internet resources that are blocked by our Internet filter may be unblocked at the request of a teacher or administrator, providing such access is appropriate for students and is consistent with the educational goals of the district and within the guidelines for acceptable use. Staff must preview any such web sites, portals or other Internet resources to ensure their compatibility to these policies and acceptable use before making such requests.

(b) Internet access can be monitored electronically through software, and all access by students and other minors is automatically logged by filtering software. Log files are kept for a period not to exceed 30 days, after which the log files may routinely be overwritten. Log files will be periodically reviewed by the system administrator, and can be viewed by parents or staff at any time.

(c) Students will be given a district email account as needed for educational use and in fact email accounts are necessary for students to access their Google account. Use of electronic mail accounts must be consistent with the educational goals of the district and within the guidelines for acceptable use. Students may use email accounts if supervised by a staff member and may only use the email account for educational purposes. This includes all forms of electronic mail, including chat rooms and instant messaging.

(d) This policy requires the permission of and supervision by the school's designated professional staff before a student may use a school account or resource to access the Internet, web portals, or other web resources, including 'social networking sites,' or use any form of electronic communications over the Internet; all such use must be consistent with the educational goals of the district and within the guidelines for acceptable use.

(e) When users access the school district system from sites off campus (i.e., from home), provisions of this policy still apply. Outside of school, it is the responsibility of the user to ensure that such use complies with all provisions of this agreement.

10. Internet Safety

As part of the High School Study Skills program and the Elementary Developmental Guidance program the District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms as well as cyber bullying awareness and response.

11. Student Web Pages

Students may be given space on the District Web server to post student-made Web pages. The content of such Web pages must be for educational purposes must be supervised by a staff member, and the content must conform to all district standards and policies.

12. Use of Mobile Learning Devices

Student use of district owned mobile learning devices (MLDs) such as laptops, netbooks, iPods, iPads, Chromebooks, etc. falls under the guidelines of this Computer Network & Internet Use Policy. Access to the internet is monitored through the district's content filtering software and all rules and expectations are applied to the use of all such devices. All applications, activity and documents stored on MLDs are the property of The Pittsville School District and subject to regular review and monitoring. Students may be allowed to take MLDs off school grounds for use at home or for other appropriate educational purposes, provided such use conforms to all appropriate school procedures & policies.

(a) Students may not:

- Modify MLDs in any way other than instructed by the administrator or other school personnel.
- Exchange MLDs with another student or share a password with anyone else or access any account belonging to other students, faculty, or staff.
- Allow other students to retain or remove MLDs from their presence.
- Apply any permanent marks, decorations, or modifications to the MLDs.
- Synchronize the MLDs with another computer outside of the school.
- Clear or disable browsing history or set password protection on the device.
- Disable the MLDs or its applications.
- Change, alter, bypass, or attempt to bypass any MLD security measures including filtered Internet

access.

- Use the device in any way or make any changes to the device which is not consistent with district policies or educational purposes.

(b) Use of the MLDs may require a few necessary tasks to keep the devices performing well:

- On-line time must be used wisely to allow equitable access for all users.
- Clean the screen often with approved cleaning towels.
- Make sure hands are clean before using.
- Keep away from food and drink.
- Charge the MLD only with the included charger and using a standard wall outlet for your power source.
- Report any software/hardware issues to your teacher as soon as possible.
- Keep the MLD in a well protected temperature controlled environment when not in use.
- Keep the MLD secure - take reasonable precautions to protect MLDs and any data stored on them from theft or damage.
- Return the MLD to the school in good condition in a timely manner, or as directed.

(c) Applications will be preinstalled on each MLD by school staff. Additional applications may be reviewed and added to facilitate academic needs. Purchasing and installing these applications is the responsibility of the school. The student user is not to install any applications not approved by their teacher or the Pittsville School District.

(d) Damage due to a determined accidental cause will be addressed by the school through normal procedures. Damage due to negligence may result in the student/parents assuming the financial responsibility of replacement of the MLD. Student use of the MLD off school grounds may be revoked at anytime by the administration.

13. Personal Electronic Devices

Pittsville School District offers wireless access in our buildings. Each time someone accesses the wireless network, s/he must agree to the terms listed below:

- Student use of devices will be at the discretion of the teacher or other district staff and must be used for educational purposes.
- Students are prohibited from using any personally owned electronic devices or electronic communication devices during instructional time (as determined by the teacher), during exam periods, in locations where there is an expectation of privacy, or when the device distracts others or interferes with the operation of the school.
- Users must follow all appropriate district policies, procedures, and computer etiquette while using any personal electronic devices on school grounds, or while connecting to the district wireless network or using network resources.
- The district will not be held liable for any damage that may occur as a result of connecting to the wireless network or any electrical power source.
- The district will not be held responsible for any physical damage, loss or theft of the device.
- The district is not obligated to supply electrical power access.
- Persons connecting devices to the wireless network agree to maintain current anti-virus software.
- The parents and/or guardians of any student bringing personal technology to school agree to be responsible for and to reimburse Pittsville Public Schools for any damage that their student may cause arising out of and relating to the use of the wireless network with his/her personal wireless device.

14. Cloud Computing & Storage

Saving documents on Internet storage sites (such as ‘Google Docs’) is known as cloud storage. The district may set up accounts for students with companies such as Google (Google Apps/Google Docs) that provide such services. Student use of any such accounts must comply with all applicable district policies, and are subject to review by teachers and staff. Use of these services shall be treated the same as if the storage or service was provided locally by the district's own servers and computer equipment, and all appropriate policies, behavior expectations, and computer etiquette will apply.

15. At-Home Access to District Technology

The District may provide staff, students, and parents with access to District technology and information through the use of home computers over the Internet in accordance with the following guidelines:

(a) Access will be made available at no charge.

(b) The District will not be responsible for:

  1) Any virus, worm, or other infestation that a home-user may obtain through District access.
  2) Any copyright violations that may be incurred through District access.
  3) Loss or damage to any equipment or software of the home-user.

(c) Any parents or students who wish to access student and/or family accounts will be provided with a login procedure, name, and password. All users must take steps to secure such passwords to prevent unauthorized access to student and/or family accounts

(d) Access to District technology for staff, students, and parents is provided as a service and not a right of users. Access can be denied for any violation of this Student Internet Safety and Technology Use Policy.

16. Disclaimer

The School District of Pittsville makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages. This includes loss of data resulting from delays, non-deliveries, or service interruptions caused by its own negligence or user's errors or omissions. The School District of Pittsville specifically denies any responsibilities for the accuracy or quality of information obtained through its services. The school district will not be responsible for financial obligations arising through unauthorized use of the school district system or the Internet. Users must agree to Indemnify and hold harmless the School District of Pittsville for claims arising out of the use of the computer network.

Update: *August 12, 2013*

Student Internet Safety and Technology Use

Policy 363.2

OPT-OUT Form

If any parent/guardian objects to or refuses to permit the District to provide Internet access, they should annually submit this form to the building principal. An account that allows access to the school networked computers and installed software, but restricts access to the Internet, will be provided.

THE SIGNATURE BELOW CERTIFIES THAT INTERNET ACCESS SHOULD BE RESTRICTED FOR THE CURRENT SCHOOL YEAR FROM THE ACCOUNTS FOR THE STUDENT(S) LISTED BELOW.

Student(s) to be restricted from Internet access:

Student Name	Grade	School

Parent or Guardian's Name:____
Please print

Signature______________________________________ Date_________________________