



Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Internet/Network
Number	815
Status	Active
Legal	1. Pol. 218 2. Pol. 233 3. Pol. 317 <a href="#">4. 24 P.S. 4604</a> <a href="#">5. 47 U.S.C. 254</a> <a href="#">6. 20 U.S.C. 6777</a> 7. Pol. 249 9. Pol. 814 <a href="#">10. 47 CFR 54.520</a> 11. Pol. 216 <a href="#">12. 17 U.S.C. 101 et seq</a> <a href="#">24 P.S. 1303.1-A</a> <a href="#">24 P.S. 4601 et seq</a> <a href="#">18 U.S.C. 2256</a> <a href="#">i-SAFE Inc.</a>
Adopted	August 12, 2014
Last Revised	November 18, 2014

### **Purpose**

The Board supports use of the Internet and other computer networks in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district, as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

This policy has been developed to:

1. Ensure security, reliability and integrity of the system.
2. Avoid situations that may cause the district to incur civil liability.
3. Maintain the image and reputation of the Wayne Highlands School District as a responsible Internet user/provider.
4. Encourage responsible use of the Internet resources and discourage practices that degrade the usability of Internet services.
5. Preserve the privacy and security of individual users subject to authorized employer review and legal processes.

### **Authority**

The electronic information available to students and staff does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

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

The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources.[1][2][3]

The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action.

The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources.

The district shall inform staff, students, parents/guardians and other users about this policy through employee student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon request.[\[4\]](#)

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use. Student user agreements shall also be signed by a parent/guardian.

The Board shall establish a list of materials, in addition to those stated in law, that are

inappropriate for access by minors.[\[5\]](#)

### **Delegation of Responsibility**

The district shall make every effort to ensure that this resource is 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 Superintendent/Director of Technology shall have the authority to determine what inappropriate use is.

The Superintendent/Director of Technology shall be responsible for implementing technology and procedures 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:[\[6\]](#)[\[5\]](#)

1. Utilizing a Children's Internet Protection Act (CIPA) compliant 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**

Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

### **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. Specifically, the following uses are prohibited:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Nonwork- or nonschool-related work.

4. Product advertisement or political lobbying.
5. Bullying/Cyberbullying.[7]
6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. Access to obscene or pornographic material or child pornography.
9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
10. Inappropriate language or profanity.
11. Transmission of material likely to be offensive or objectionable to recipients.
12. Transmission of any material that, at the Board's sole discretion, is unlawful, threatening, abusive, libelous, hateful, or encourages conduct that would constitute a criminal offense, give rise to civil liability, or otherwise violate any local, state, federal or international law.
13. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
14. Impersonation of another user, anonymity, and pseudonyms.
15. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
16. Loading or using of unauthorized games, programs, files, or other electronic media.
17. Disruption of the work of other users.
18. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
19. Quoting of personal communications in a public forum without the original author's prior consent.

### 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 access another person's account or use a computer that has been logged in under another student's or employee's name.

3. Any attempt to circumvent user authentication or security of any host or network is prohibited.
4. Communications may not be encrypted so as to avoid security review.
5. Users who violate systems or network security shall incur criminal or civil liability, as well as possible suspension or discharge. The Wayne Highlands School District will cooperate fully with any investigation of security and or network violations.
6. Only office personnel shall have access to the office computers.
7. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

### Email

All uses of the email system must be consistent with the mission of the Wayne Highlands School District. All staff are to check their email account daily, and appropriate responses are expected within a reasonable period of time (one (1) Business Day). Guidelines for email use include, but are not limited to, the following:

1. Harassment, whether through language, frequency, or size of messages is prohibited.
2. Reposting of personal communications without the author's consent is prohibited.
3. Employees may not send email to any person who does not wish to receive it. If a recipient asks to stop receiving email, the employee must not send that person any further email.
4. Employees are prohibited from sending unsolicited bulk mail messages (e.g., junk mail, spam, etc.).
5. Forging of header information in any deceitful manner is prohibited.
6. No chat rooms are permitted.
7. Personal email is prohibited on company paid time.

### Consequences for Inappropriate Use

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

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

General rules for behavior and communications apply when using the Internet, in addition to

the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Vandalism will result in cancellation 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

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.[\[12\]](#)[9]

### 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.

Any district computer utilized by students shall be routed through a Children's Internet Protection Act (CIPA) compliant blocking/filtering software.

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is prohibited by this policy.[\[4\]](#)

Internet safety measures shall effectively address the following:[\[5\]](#)[\[10\]](#)

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.

### Video Surveillance and Photo Usage

The safety of our faculty, staff, and students is very important to the school district. The school district does monitor and record digital video of its campus and buildings interiors every minute of every hour of every day through the use of video surveillance on its network.

The district reserves the right to use video surveillance in cooperation with law enforcement, or other types of investigations. We also reserve the right, unless requested not to, by faculty,

staff, or student to publish photos of person or persons on our website, yearbook, and other types of digital means with the concept of security and safety in mind at all times.[11]

## Education

We believe, as the Wayne Highlands School District, in educating our students on this policy, as well as Internet safety. By teaching students responsible behavior, asking them to sign an agreement, and providing written descriptions of the consequences for wrongful action, students develop a sense of responsibility and ownership for their online experience.

The building administrator/Director of Technology is responsible for providing education to our faculty, staff, and students in the following:

1. Educate parents about their children's use of the Internet.
2. Educate about the risks peculiar to computer communication.
3. Educate about rules for efficient, ethical, legal computer/network use.
4. Educate about the safe and appropriate computer social behavior.
5. Educate about the use of available and unavailable services.

Specifically, the mandatory Internet safety education must include lessons on cyberbullying awareness and response, as well as teaching appropriate online behaviors for students on social networking sites and in chat rooms.[5]

The Children's Internet Protection Act (CIPA) requires, incorporating the new law enacted by Congress that imposes new requirements on any school or library that receives funding for Internet access or internal connections from the E-Rate Program.

[815-Attach.docx \(13 KB\)](#)

Last Modified by Heather Masshardt on July 16, 2015