Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of the Electronic Communications Systems and Network
Code	815
Status	Active
Adopted	December 14, 2009
Last Revised	April 8, 2013

Purpose

Whitehall-Coplay School District provides employees and students with access to the district's electronic communications systems and network, which includes Internet access, whether wired or wireless, or by any other means.

The electronic communications systems and network provide vast, diverse and unique resources. The Board will provide access to the district's network and systems and to the Internet for staff members and for students, in order to access information, for research, and for collaboration to facilitate learning and teaching.

For users, the district's network and electronic communications systems are to be used primarily for education-related purposes and performance of job duties. Incidental personal use of school computers shall be permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system users. Personal use must comply with this policy and all other applicable policies, procedures and rules, and must not damage the school's hardware, software, computer or electronic communications systems. Students may only use the network and electronic communications systems for educational purposes.

Definitions

Access to the Internet - a computer shall be considered to have access to the Internet if the computer is equipped with a modem or is connected to a computer network that has access to the Internet.[1]

Child Pornography - any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:[8]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct.

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Computer - includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer. **Computer** includes, but is not limited to: desktop, notebook, powerbook, tablet PC or laptop computers; specialized electronic equipment used for students' special educational purposes; global position system (GPS) equipment; personal digital assistants (PDAs); cell phones, with or without Internet access and/or recording and/or camera and other capabilities, mobile phones, or wireless devices; beepers; and any other such technology developed.[1]

Electronic Communications Systems - any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes. Further, **an electronic communications system** means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, but are not limited to: the Internet; intranet; electronic mail services; GPS systems; cell phones with or without Internet access and/or recording, camera, and other capabilities; and PDAs.

Educational Purpose - includes use of the network and electronic communications systems for classroom activities, professional or career development, and to support the district's curriculum, policy and mission statement.

Harmful to Minors - any picture, image, graphic image file or other visual depictions that:[1][12][2]

1. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion.

2. Depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals.

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

Incidental Personal Use - use by an individual employee for occasional, personal communications. Personal use must comply with this policy and all other applicable 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 his/her use is private. The district reserves the right to monitor access and use of its network and electronic communications systems.

The School District Network - all components necessary to effect its operation, including, but not limited to: computers; copper and fiber cabling; wireless communications and links; equipment closets and enclosures; network electronics; telephone lines; printers and other peripherals; storage media; software; and other computers and/or networks to which the school district network may be connected, such as the Internet or those of other institutions.

Minor - for purposes of compliance with the Children's Internet Protection Act (CIPA), an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean the age of minority as defined in the relevant law.[1][2]

Obscene - analysis of the material meets the following elements:[9]

1. The average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

2. The subject matter depicts or describes, in a patently offensive way, sexual conduct specifically described in the law to be obscene.

3. The subject matter taken as a whole lacks serious literary, artistic, political, educational or scientific value.

Sexual Act and Sexual Contact - as defined at 18 U.S.C. § 2246(2) and at 18 U.S.C. § 2246(3) and 18 Pa. C.S.A. § 5903.[9][10]

Technology Protection Measure(s) - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.[12][2]

Visual Depictions - undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words. [8]

Authority

Access to the district's electronic communications systems and networks through school resources is a privilege, not a right. Inappropriate, unauthorized, and illegal use may result in the revocation of those privileges and/or appropriate disciplinary action.

The electronic communications systems, networks, and user accounts are the property of the district, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity. The district will cooperate fully with Internet Service Providers, local, state and federal officials in any investigation concerning or related to the misuse of the network and electronic communications systems.

It is often necessary to access user accounts in order to perform routine maintenance and security tasks; system administrators have the right to access, by interception, the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Electronic communications systems and network users have only a limited expectation of privacy in the contents of their personal files or any of their use of the district's network or systems. The district reserves the right to track, log and monitor network and system use and to monitor and allocate fileserver space.

The district reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through software blocking or general policy. Specifically, the district operates and enforces technology protection measure(s) that monitor and track online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet. **Inappropriate matter** includes, but is not limited to, visual, graphic, text and any other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, terroristic and advocates the destruction of property. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult to access bona fide research or for another lawful purpose.[1][2]

The district reserves the right to restrict or limit usage of lower priority network, electronic communications systems and computer uses when network and computing requirements exceed available capacity according to the following priorities:

1. Highest - uses that directly support the education of the students.

2. Medium - uses that indirectly benefit the education of the students.

3. Lowest - uses that include reasonable and limited educationally-related interpersonal communications and incidental personnel communications.

4. Forbidden - all activities in violation of this policy.

The district additionally reserves the right to:

1. Determine which network and electronic communications systems services will be provided through district resources.

2. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail.

3. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time.

4. Log Internet, network, and electronic communications systems use by students and staff.

5. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable policies occurs or state or federal law is violated, including but not limited to those governing network use, copyright, security, discipline and vandalism of district resources and equipment.

Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory, inaccurate, obscene, lewd, vulgar, rude, harassing, violent, inflammatory, threatening, terroristic, hateful, bullying, profane, pornographic, offensive, and illegal, can be accessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the district cannot completely block access to these resources.

Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in suspension of network and electronic communications systems privileges and disciplinary action as outlined in appropriate Board policies.[3][4]

The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.[2]

Delegation of Responsibility

The Superintendent and/or designee will serve as the coordinator to oversee the district's network and electronic communications systems and will work with other regional or state organizations as necessary.

The Superintendent and/or designee will approve activities, provide leadership for proper training in the use of the network and electronic communications systems and the requirements of this policy, establish a system to ensure adequate supervision of the network and electronic communications systems, maintain executed user agreements, and be responsible for interpreting the district's Acceptable Use of the Electronic Communications Systems and Network Policy.

The Superintendent and/or designee will establish a process for setting up individual accounts, set quotas for disk usage on the system, establish a retention schedule, and establish the district's virus protection process.

Unless otherwise denied for cause, student access to the Internet, e-mail, or other network and electronic communications systems resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop

the skills and judgment required to make effective and appropriate use of these resources. All users have the responsibility to respect the rights of all other users within the district and district networks, electronic communications systems, and throughout the Internet, and to abide by the rules established by the district and its Internet Service Provider.

Guidelines

Limitation of Liability

The electronic information available to students and staff does not imply endorsement of the content by the district, nor does the district guarantee the accuracy of information received via the Internet. The district shall not be responsible for any information that may be lost, damaged, delayed, misdelivered, or unavailable when using the network and electronic communications systems. Neither shall the district be responsible for material that is retrieved by the Internet, or the consequences that may result from them. The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet, network, and electronic communications systems. In no event shall the district be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the Internet, network and electronic communications systems.

Access to the Network and Electronic Communications Systems

Network and electronic communications systems user accounts will be used only by authorized owners of the accounts for authorized purposes.

An account will be made available according to a procedure developed by appropriate district authorities.

The district's Acceptable Use of the Electronic Communications Systems and Network Policy will govern all use of the district's network and electronic communications systems. Student and staff use of the network and electronic communications systems will also be governed by the other relevant policies.

Types of services include, but are not limited to:

1. **World Wide Web** – District employees and students will have access to the web through the district's networked computers and electronic communications systems as needed.

2. **E-Mail** – District employees will be provided with an individual account as needed.

3. **Guest Accounts** – Guests may receive an individual account with the approval of the Superintendent and/or designee if there is a specific, district-related purpose requiring such access. Use of the electronic communications system by a guest must be specifically limited to the district-related purpose.

Parental Notification and Responsibility

The district will notify the parents/guardians about the district's network and electronic communications systems and the policies governing their use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the district to monitor and enforce a wide range of social values in student use of the Internet. Further, the district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children.

The district will encourage parents/guardians to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the district's system. Parents/Guardians are

responsible for monitoring their children's use of the district's networks when they are accessing the system.

Prohibitions

The use of the Internet computer network and electronic communications systems for illegal, inappropriate, unacceptable, or unethical purposes by students or employees is prohibited. Such activities engaged in by all users are strictly prohibited and illustrated in this policy. The district reserves the right to determine if any activity not stated in this policy constitutes an acceptable or unacceptable use of the network and electronic communications systems.

These prohibitions are in effect any time district resources are accessed whether in school, directly from home, or indirectly through another Internet Service Provider.

General Prohibitions –

It is prohibited to use the network and electronic communications systems to/for:

1. Nonwork or nonschool related communications, except for employee use when in compliance with this policy's definition of incidental personal use.

2. Access material that is harmful to minors, indecent, obscene, pornographic, child pornographic or terroristic.

3. Transmit material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, inaccurate, obscene, lewd, hateful, harassing, violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.

4. Cyberbullying another individual.[5][6]

5. Access or transmit gambling or pools for money, including but not limited to basketball and football, or any other betting or games of chance.

6. Participate in discussion or news groups which cover inappropriate and/or objectionable topics or materials, including those which conform to the definition of inappropriate matter in this policy.

7. Send terroristic threats, hate mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.

8. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (online, real-time conversations) that are not for school-related purposes or required for staff members to perform their job duties.

9. Facilitate any illegal activity.

10. Communicate through email for noneducational purposes or activities, unless it is for an incidental personal use as defined in this policy. The use of email to mass mail noneducational or nonwork related information is expressly prohibited (for example, the use of the "everyone" distribution list, building level distribution lists, or other email distribution lists to offer personal items for sale is prohibited).

11. Commercial, for-profit, or business purposes (except where such activities are otherwise permitted or authorized under applicable Board policies), unauthorized fundraising or advertising on behalf of the district and nonschool district organizations, reselling of district computer resources to nonschool district individuals or organizations, or unauthorized use of

the district's name. **Commercial purposes** is defined as offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for the district's purchase of goods or supplies through the district's system.

12. Political lobbying.

13. Advertising of any kind, unauthorized fundraising or unauthorized use of the district's name will not be permitted on the Internet or email, or any other online service.

14. Anything that results in a copyright violation.[7]

15. Install, distribute, reproduce or use copyrighted software on district computers, or the copying of school district software to unauthorized computer systems.

16. Install computer hardware, peripheral devices, network hardware or system hardware.

17. Intentionally infringing upon the intellectual property rights of others.

18. Use of the network and electronic communications systems to commit plagiarism.

19. Making available material or information the possession or distribution of which is illegal.

20. Unauthorized access, interference, possession, or distribution of confidential or private information including messages sent to them privately without permission of the person who sent the message.

21. Intentionally compromising the privacy or security of electronic information.

22. Using the systems to send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the district's business or educational interest.

23. Sending unsolicited commercial electronic mail messages, also known as spam.

24. Posting professional web pages without administrative approval.

25. Access to materials, images or photographs that are obscene, pornographic, lewd or otherwise illegal.

Access and Security Prohibitions –

Users must immediately notify the Superintendent and/or designee if they have identified a possible security problem. The following activities related to access to the district's computer network, electronic communications system 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, electronic communications systems, 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 a communication originally received from another person or computer with the intent to deceive.

6. Use of district resources 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.

Operational Prohibitions –

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of computer, electronic communications systems, or network accounts, services or equipment of others, including, but not limited to, the propagation of computer worms and viruses, the sending of electronic chain mail, and the inappropriate sending of broadcast messages to large numbers of individuals or hosts. In other words, the user may not hack or crack the network or others' computers, whether by parasiteware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage computers, the network, or any component of the network, or strip or harvest information, or completely take over a person's computer, or "looking around."

2. Altering or attempting to alter files, system security software or the systems without authorization.

3. Unauthorized scanning of the electronic communications systems and network for security vulnerabilities.

4. Attempting to alter any district computing or networking components (including, but not limited to fileservers, bridges, routers, or hubs) without authorization or beyond one's level of authorization.

5. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or retransmission of any computer, electronic communications systems, or network services, whether wire or wireless.

6. Connecting unauthorized hardware and devices to the electronic communications systems and network.

7. Loading, downloading, or use of unauthorized games, programs, files, or other electronic media.

8. Intentionally damaging or destroying the integrity of electronic information.

9. Intentional destruction of the district's computer hardware or software.

10. Intentionally disrupting the use of electronic communications systems, networks or information systems.

11. Negligence leading to damage of the district's electronic information, computing, electronic communications systems, or networking equipment.

12. Failure to comply with requests from appropriate teachers or administrators to discontinue activities that threaten the operation or integrity of computers, systems, or networks.

Content Guidelines

Information electronically published on the district's electronic communications systems and network, including, but not limited to the school district's World Wide Web pages, shall be subject to the following guidelines:

1. Published documents or videoconferences may not include a child's phone number, street address, or box number, name (other than first name) or the names of other family members.

2. Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent.

3. Documents, web pages, electronic communications, or videoconferences may not contain objectionable material or point directly or indirectly to objectionable materials.

4. Documents, web pages and electronic communications must conform to Board policies and guidelines, including the copyright policy.[7]

5. Documents to be published on the World Wide Web must be edited and approved according to district procedures before publication.

Due Process

The district will cooperate fully with the district's Internet Service Provider, local, state, and federal officials in any investigation concerning or relating to any illegal activities conducted through the district's electronic communications systems and network.

The district may terminate the account privileges by providing notice to the user.

Search and Seizure

User violations of the district's Acceptable Use of the Electronic Communications Systems and Network Policy or the law may be discovered by routine maintenance and monitoring of the district system or by any method stated in this policy, pursuant to any legal means.

The district reserves the right to monitor any electronic communications, including but not limited to Internet access and e-mails. Students and employees should have only a limited expectation of privacy in electronic communications, even when used for personal reasons.

Copyright Infringement and Plagiarism

Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through district resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Teachers will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements.

Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the district's computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap, browsewrap, and electronic software downloaded from the Internet.[11][7]

District guidelines on plagiarism will govern use of material accessed through the district's electronic communications systems and network. Users will not plagiarize works that they find on the Internet. Teachers will instruct students in appropriate research and citation practices.

Selection of Material

Board policies on the selection of materials will govern use of the Internet.

When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the

materials and websites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

School District Website

The district will establish and maintain a website and will develop web pages that will present information about the district, under the direction of the Superintendent.

Safety

To the greatest extent possible, users of the Internet, electronic communications systems, and network will be protected from harassment or unwanted or unsolicited communication. Any user who receives threatening or unwelcome communications shall immediately bring them to the attention of the Superintendent and/or designee.

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, parasiteware, cookies, or use the network in any way to invade one's privacy. Additionally, the user may not disclose, use or disseminate personal information to other users about students or employees on the network, including chat rooms, email, Internet, etc. (examples include, but are not limited to, student 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 address, telephone number, school address, and work address.

Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.[1][2]

Internet Safety Education

Provisions shall be maintained through the curriculum department to provide for formal online safety education to all students. Online Safety Education shall be administered in specific curricular areas in all grades K-12 in varying venues to assure that all minors are mandatorily educated. Education shall include (but is not limited to) appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response. Documentation of the online safety education shall be maintained by methods prescribed by the curriculum department.[6]

Internet safety measures shall effectively address the following:[2]

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.

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

Documents or videotapes may not include information that reveals the physical location of a student at a given time.

Consequences for Inappropriate Use

Students and employees must be aware that violations of this policy or unlawful use of the computers, Internet or the district's electronic communications systems and networks may result in disciplinary action or loss of privileges.

Loss of Internet, electronic communications systems, and network access could be one of the disciplinary actions; however, this policy incorporates all other relevant Board policies such as, but not limited to, student and employee discipline policies, copyright policy, property policy, curriculum policies, and unlawful harassment policies.

General rules for behavior and communications apply when using the Internet, electronic communications system and network, in addition to the stipulations of this policy. Loss of access and a variety of other disciplinary actions, including but not limited to oral or written reprimands, suspension with or without pay, and dismissal may result from inappropriate use on a case-by-case basis. For example, disciplinary action may be taken for inappropriate language or behavior in using the district's resources.

The network user shall be responsible for damages to network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.

Violations as described in this policy may be reported to the district and appropriate legal authorities, whether the Internet Service Provider, local, state, or federal law enforcement. The district will cooperate to the extent legally required with authorities in all investigations.

Vandalism will result in cancellation of access to the district's Internet, electronic communications systems and network resources and is subject to discipline.

Legal

1. 20 U.S.C. 6777
2. 47 U.S.C. 254
3. Pol. 218
4. Pol. 317
5. 24 P.S. 1303.1-A
6. Pol. 249
7. Pol. 814
8. 18 U.S.C. 2256
9. 18 Pa. C.S.A. 5903
10. 18 U.S.C. 2246
11. 17 U.S.C. 101 et seq
12. 20 U.S.C. 9134

24 P.S. 4601 et seq

Pol. 103

Pol. 104

815-Attach.doc (27 KB)