Williamsburg Community School District

Policy Guides

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET

ADOPTED: 8/20/96, 1/19/01,

REVISED: 2/16/04, 10/20/09, 8/19/10

FIRST READING: 6/28/11

814(a). ACCEPTABLE USE OF INTERNET

1. 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.

The **District Network** includes all local area networking and wide area networking within the school community as well as all on-line and direct-wired networking, such as the Internet, to which the school network may be linked.

2. Authority

The District does not endorse any content accessible through the use of the District Network, 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 restoring any data which is lost, damaged, or becomes otherwise unavailable while utilizing the District Network.

The District reserves the right to re-image any District computer at its sole discretion. The District also reserves the right to examine the contents of any District computer at its sole discretion and without prior notice.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet. Users will be responsible for indemnifying the District for any and all claims, lawsuits, causes of action, damages, judgments, losses, expenses, liabilities, or costs associated with a violation of the Acceptable Use of Computer Networks Policy without limitation. All users of the District Network and District-owned computer hardware, software, and equipment shall be bound by this policy.

District network resources are subject to retrieval and review by the District at any time without prior notice to students or staff. The District reserves its right to

	inspect and examine any use of the District systems; this includes but is not limited to, a user's internet access, email transmissions, and all system registries. The district reserves the right to log network use and to monitor fileserver space utilization by district users. It may be necessary to access user accounts in order to perform routine maintenance and security tasks. The system administrator has the right to access user accounts to uphold this policy and maintain the system. The District reserves the right to remove a user account from the network to prevent violation of this policy or any unauthorized or illegal activity. Student access to the Internet other than through District network resources and equipment is prohibited on school property. The hardware, software, messages transmitted, and documents created on the network are the property of the District. Network users should be aware that computer files and communications over the District network, including email and voicemail, are not private. **Under no circumstances shall there be any expectation of privacy when using any District systems.** The District has the right to supervise the use of school property, including the hardware, software, messages transmitted, and documents created on the network. The Board establishes that network use is a privilege, not a right. Inappropriate, unauthorized and illegal use will result in the cancellation of these privileges and/or appropriate disciplinary action and criminal or civil prosecution where appropriate.
P.L. 106-554 Sec. 1732	The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.
3. Delegation of Responsibility	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 both the district and on the Internet generally. The building administrator shall have the authority to determine what is inappropriate use.
P.L. 106-554 Sec. 1711, 1721	The Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the District's network and equipment, including District computers, are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:

	1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene as defined by law and in this policy, 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.
4. Guidelines	All students and staff will be permitted to use District network resources in furtherance of the mission of the School District. An internet/computer network exemption form shall be made available to parents or guardians that choose to prohibit their child's internet access. As the student matriculates from one school building to the next, the parent/guardian shall submit the internet/network exemption form if they choose to continue to prohibit their child's access to these resources. This policy shall be published or referenced annually in the student and staff handbooks. 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. Users are not to access the District's intranet, owned or leased technological resources, or internet access while utilizing another User's personal access information. Users are given their own personal ID. Users are responsible for maintaining the privacy of their passwords. Users are responsible for their own individual accounts and should take reasonable precautions to prevent others from using their account. Users must log off or lock the computer when finished or when leaving their work station. Users are only to sign on to the network with the ID assigned to them. Users will represent only themselves on the network and will only attempt to modify files or passwords belonging to them. Misuse of passwords, unauthorized copying of another's work, and attempting to access files maintained by others is strictly forbidden. When a user is no longer employed by the District or is no longer a student of the District, their account will be deleted or suspended. Special circumstances may be approved by the Superintendent for accounts to be maintained for a defined period of time. <u>Prohibitions</u> 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. The use of the District systems for illegal, inappropriate, or unethical purposes by students or employees is **strictly** prohibited.

Specifically, the following uses are prohibited:

1. Any illegal activity.

2. Engaging in activity that is for commercial, for-profit, or for any other business purpose (except where such activities are otherwise permitted or authorized under applicable District policies); conducting unauthorized fundraising or advertising on behalf of the District, conducting fundraising or advertising on behalf of any non-school organization(s); reselling of District computer resources to individuals or organizations who are not related to the District; or use of the District's name in any unauthorized manner that would reflect negatively on the District, its employees, or students. "Commercial purposes" are defined as offering or providing goods or services or purchasing goods or services for personal use.
3. Use that is not school or work related, except for incidental personal use. E-mail is not to be used for the mass mailing of non-educational or non-work related information or for the sending of unsolicited commercial electronic mail messages, commonly known as spam.

4. Product advertisement or political lobbying.

5. District systems shall not be used for bullying/cyberbullying; sending terroristic threats or hate mail; harassing communications; making discriminatory remarks; and any and all other harassing, offensive, or inflammatory communications.

6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials in violation of copyright laws or "fair use" guidelines.

7. Accessing, opening, obtaining, transmitting, or distributing any materials, images, videos, text, or photographs that are obscene, pornographic, lewd, constitute child pornography as defined herein, or are otherwise illegal or determined to by the Board to be inappropriate for children.

8. Access by students, faculty, and guests to material that is harmful to minors or is determined to be inappropriate for minors in accordance with Board policy.

9. Use of any inappropriate language or profanity.

10. Accessing, distributing, e-mailing, transmitting, downloading, or opening any material, images, videos, text, or photographs likely to be offensive or objectionable to recipients or viewers, including but not limited to that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful,

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, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic, and/or otherwise illegal.

11. Accessing e-mail programs and accounts, including web-based e-mail providers, other than the approved District e-mail program, is prohibited on the network. All school-related correspondence must be sent via the e-mail account provided by the District.

12. Impersonation of another user, maintaining anonymity, using pseudonyms, or gaining or attempting to gain network access through fraudulent means.

13. Access and use of online "gaming" sites (except for approved educational purposes.

14. Loading or using of unauthorized games, programs, files, music, or other electronic media, pirated software, and peer-to-peer file-sharing software. Student and guest network users will not download files unless instructed to do so by a teacher who has obtained authorization from the Superintendent or his/her designee.

15. Disrupting the work of other users.

16. Accessing or transmitting any form of gambling, including but not limited to, basketball and football pools, online poker websites, and any other form of betting, gambling, or games of chance.

17. Quoting of personal communications in a public forum without the original author's prior consent.

18. Accessing "social networking" sites for non-curricular purposes, including participation in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (on-line, real-time conversations) that are not for school-related purposes or required for employees to perform their job duties.

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

20. Accessing, interfering, possessing, or distributing confidential or private information without permission from the District administration, e.g. accesing another student's account to obtain their grades. Users may not violate the privacy or security of electronic information contained on the network.

21. Distributing or publishing a password, identifying code, personal identification number, username, or any other confidential information about a computer, computer system, network, or email account or database.

Violation of any of the above provisions in this policy may result in the suspension, termination of a user's privilege to technology resources and/or a restriction of the user's privileges. All users should understand that if they commit any violation of this policy, their access privileges may be suspended or revoked, school disciplinary action will be taken, and/or appropriate legal action may be instituted.

Materials stored on individual computers and file servers is the property of the educational agency and is, therefore, accessible by the educational agency at any time and can be disclosed to whomever the agency desires at any time. Electronic files and communication are subject to disclosure as deemed necessary to maintain compliance.

<u>Operational Prohibitions</u>

The following operational activities and behaviors are prohibited:

1. Interference with or disruption of the District systems, network accounts, services, or equipment through, but not limited to, the propagation of computer worms and viruses; Trojan horse and trapdoor program code; the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of broadcast messages to large numbers of individuals or hosts.
2. The User may not hack or crack the network or others' computers, whether by parasighteware or spyware designed to steal information; viruses; worms; other hardware or software designed to damage District systems, or any component of the network, to strip or harvest information, to completely take over a person's computer, or to allow the intruder to "look around."
3. Tampering with network hardware or software.
4. Gaining unauthorized access into other protected areas of the network.
5. Attempting or actually by-passing the District's filtering software.
6. Intentionally vandalizing or destroying network files or data belonging to or used by others, or other behavior that interferes with the function of the District network.
7. Altering or attempting to alter files, system security software, or any District systems without authorization.
8. Unauthorized scanning of the District systems for security vulnerabilities.
9. 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.
10. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or retransmission of any computer,

electronic communications system, or network services, whether wired, wireless, cable, or by other means.

11. Connecting unauthorized hardware and devices to the District systems
12. Loading, downloading, or use of unauthorized software, games, programs, files, or other electronic media, including but not limited to downloading music files, pirated software, and peer-t-pear file-sharing software.

Any user who violates the prohibitions of this section will be strictly liable for any damage to District systems without regard to intent to cause harm. The act taken in violation of this section of the policy shall be sufficient to establish the individual's intent to cause harm.

Disclaimer

The District makes no warranties of any kind, whether express or implied, for the service it is providing. The District is not responsible and will not be responsible for any damages, including loss of data resulting from delays, nondeliveries, missed deliveries, or service interruption. Use of any information obtained through the District's computers is at the user's risk. The District disclaims responsibility for the accuracy or quality of information obtained through the Internet or e-mail.

Other Communications

Other communications include but are not limited to: e-mail, chatrooms, discussion boards, blogging, instant messages, journaling, or any other communication tool.

1. Users may be granted District e-mail accounts for work related and incidental personal use.
2. Incidental personal use of school computers is permitted as long as such use does not interfere with the user's job duties and performance, with the system operations, or other system users. "Incidental personal use" is defined as use by an individual employee for occasional personal communications. Users are reminded that such personal use must comply with this policy and all other applicable policies and procedures. Further, even incidental personal use is subject to District oversight and review at any time.
3. Electronic communication is subject to District review at any time. No electronic communication sent through the District system is private. Under certain circumstances, such as a result of investigations, subpoenas, or lawsuits, the District may be required by law to disclose the contents of electronic communications to a third party.
4. Access to e-mail programs or web-based e-mail providers, other than the approved District e-mail program is prohibited on the District systems. All school-related correspondence msut be sent via the e-mail account provided by the District.
5. Other types of communication programs are to be used for educational purposes

only and must be connected to the curriculum. All communication programs which the faculty wishes to use for educational purposes must be reviewed and approved by the Superintendent or his/her designee.

Security

The District has several safeguards in place to protect students from accessing information that is not suited for educational purposes. The security of District systems are protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To the greatest extent possible, internet filtering software is in place to monitor and block inappropriate material from access by students and staff. The Superintendent or his/her designee may authorize the disabling of filtering software during use by an adult to enable access for bona fide research or other lawful purposes. To protect the integrity of the system, the following guidelines shall be followed:

1. Individuals should be careful with the use of passwords and shall not reveal their passwords to another individual

2. Users are not to use a computer that has been logged in under another student's or employee'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 network.

4. Users may be required to change their passwords at any time and should change their passwords regularly.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Deliberate and willful acts will be construed so as to include any accidental infection or other harm resulting from the intentional violations of any provision of this policy, even if infliction of the infection or other harm was not the intended goal of the activity.

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.

As stated in other sections of this policy, access to the Internet and District systems

	and technology is a privilege, not a right; and inappropriate, unauthorized, and/or illegal use will result in the cancellation of access privileges and appropriate disciplinary/legal action. Any act of vandalism will be subject to an appropriate penalty as provided for herein without regard to the user's intent or purpose in carrying out the prohibited activity. The District reserves the right to prosecute and hold liable any User whose activities in violation of this policy or acts of vandalism result in damage to the District's systems. Users whose actions inflict damage upon the District's systems shall be held liable for any damages resulting from their acts in violation of this policy. Vandalism will result in the immediate cancellation of access privileges and the District reserves the right to prosecute and hold the User liable fore any damages, foreseen or unforeseen, resulting from the User's acts of vandalism. Under Pennsylvania law it is a crime to access, alter, or damage any computer system, network, software, or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. It is also unlawful to knowingly and without authorization disclose a password to any computer system or network, to gain unauthorized access to a computer or to interfere with the operation of a computer, or to alter any computer software without authorization. Violations of these sections of Pennsylvania law are a felony punishable by a fine of up to $15,000 and up to seven (7) years of imprisonment. Disclosure of a password to a computer system or network knowingly and without authorization is a misdemeanor punishable by a fine up to $10,000 and imprisonment of up to five (5) years. Users are placed on notice that their actions in violation of this policy and any applicable law, can and will, where appropriate, result in criminal and/or civil prosecution. <u>Copyright</u>
P.L. 94-553 Sec. 107 Pol. 814	Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the District resources. 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. All Users must comply with the mandates of Copyright law and shall not use copyrighted materials illegally or without a proper license, nor shall any User commit an act of plagiarism. The illegal use of copyrighted materials is strictly prohibited. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and will comply with license agreements. Violations of copyright law may be a felony and the law allows a court to hold individuals personally responsible for copyright infringement. The District does not, and will not, tolerate violations of federal copyright law. Therefore, any user

violating federal copyright law does so at their own risk and assumes all liability for their actions.

Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material, distributing copyrighted materials over computer networks, and deep-linking and framing into the conten of others' websites. 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—shrinkwrap, clickwrap, browsewrap, and electronic software downloaded from the internet.

District guidelines regarding plagiarism will govern the use of material access through the District systems. Users will not plagiarize works that they find and acts of plagiarism are strictly prohibited and will be subject to appropriate punishment. Teachers will instruct students in appropriate research and citation practices.

Due Process

The District will cooperate with the District's ISP, local, state, and federal officials to the extent legally required in investigations concerning or relating to any illegal activities conducted through the District's systems.

If students or employees possess due process rights for discipline resulting from the violation of this policy, they will be provide such rights in accordance with the law.

The District may terminate the account privileges of any user without prior notice.

Search and Seizure

Violations of this policy, any other District policy, or the law may be discovered by routine maintenance and monitoring of the District system, or any method stated in this policy, or pursuant to any legal means.

The District reserves the right to monitor, track, log, and access any electronic communications, including but not limited to, Internet access and e-mails, at any time for any reason. Users have no expectation of privacy in their use of the District systems and technology, even when used for incidental personal reasons. Further, the District has reserved the right to access any personal technology device of users brought onto the District's premises or at District events, connected to the District network, containing District programs, or containing student data in order to ensure compliance with this policy and other District policies, to protect the District's resources, and to comply with all applicable laws.

	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, e-mail, Internet, etc. Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
P.L. 106-554 Sec. 1732	Internet safety measures shall effectively address the following: 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 minor's access to materials harmful to them. 6. Educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.
5. 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 network that has access to the Internet, whether by wire, wireless, cable, or any other means. **Inappropriate Matter**—Any material that, in addition to items defined under "Harmful to Minors," constitutes a safety/security concern, creates a hostile or intimidating environment, or violates any existing District Policy or the Student Code of Conduct. **Incidental Personal Use**—Use of District systems by an individual employee for occasional personal communications is permitted. Personal use must comply with this policy and all other District policies, procedures and rules, as well as Internet Service Provider (ISP), local, state and federal laws and may not interfere with the employee's job duties and performance, with system operations, or with other

	system users, and must not damage the District's systems. Under no circumstances should the employee believe their use is private. The District reserves the right to monitor, track, access, and log the use of its systems at any time. **Network**—A system that links two or more computer systems, including all components necessary to effect the 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 District network may be connected, such as the Internet, the Internet2, or those of other institutions. **Obscene**—Material will be considered obscene when it meets the following elements: a. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest; b. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene; and c. Whether the work taken as a whole lacks serious literary, artistic, political, or scientific value. **User**—Any student, staff or guest who accesses any District network resources or facilities, including but not limited to, District computers, the District network, District hardware, District software, accesses the Internet through the District's connection, or any other District systems. **Vandalism**—Any malicious attempt to harm or destroy the District's computers, data, applications, and/or network functionality or the data, applications, or functionality of another user's computer. This includes, but is not limited to the uploading or creation of computer viruses. References: Child Internet Protection Act – 24 P.S. §§ 4601, *et. seq*. U.S. Copyright Law – 17 U.S.C. §§ 101 *et. seq*. Enhancing Education Through Technology Act of 2001 – 20 U.S.C. § 6777 Internet Safety – 47 U.S.C. § 254
P.L. 94-553 Sec. 107 P.L. 106-554 Sec. 1711, 1721, 1732 20 U.S.C. Sec. 6777	

Board Policy 814	State Board of Education Regulations – 22 Pa. Code § 403.1 Board Policy 814