UNIONVILLE-CHADDS FORD SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS

ADOPTED: November 17, 2003

REVISED: June 18, 2012

815. ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEMS

1. Purpose

Unionville-Chadds Ford School District ("District") provides employees and students with access to the District's electronic communication systems, which includes Internet access, whether wired or wireless, or by any other means.

The Internet is an electronic communications network which provides vast, diverse and unique resources. The Board will provide access to the district's networks and to the Internet for staff members and for students having the consent of their parents/ guardians to locate material to facilitate learning and teaching through interpersonal communications, access to information, research, and collaboration, i.e., to foster the educational purposes and mission of the school District.

For students, the District's network shall solely be used for educational purposes. The Board will also provide access to staff and faculty for accomplishing District business. For staff, the District's networks are to be used primarily for school-related purposes and performance of job duties. Incidental personal use of school computers is permitted 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 violate any of the rules contained in this policy, and must not damage the school's hardware, software, or computer communications systems.

School librarians, teachers, and staff will work together to help students develop critical thinking skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use information to meet educational goals that are consistent with the District's strategic plan and student learning outcomes.

2. Definitions
20 U.S.C.
Sec. 6801

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 which has access to the Internet.

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:

	1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 2. Such visual depiction is, or appears to be, 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; or
18 U.S.C. Sec. 2256	4. Such visual depiction is advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.
20 U.S.C. Sec. 6801	**Computer** – Includes any hardware, software, or other technology attached or connected to, installed in, or otherwise used in connection with a computer. **The District network** – All components necessary to effect its operation, including, 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 or those of other institutions. **Educational purpose** – Includes use of the system 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. 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, and
20 U.S.C. Sec. 6801 47 U.S.C. Sec. 254 (h)	3. Taken as a whole lacks serious literary, artistic, political, 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 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 their use is private, the District reserves the right to monitor access and use of its network.
20 U.S.C. Sec. 6801 47 U.S.C. Sec. 254(h)	**Minor** – An individual who has not attained the age of seventeen (17).
18 U.S.C. Sec. 1460	**Obscene** – Analysis of the material meets the following elements: whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest; 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 whether the work taken as a whole lacks serious literary, artistic, political, or scientific value.
18 U.S.C. Sec. 2246(2) 18 U.S.C. Sec. 2246(3)	**Sexual Act and Sexual Contact** – As defined at 18 U.S.C. § 2246(2), and at 18 U.S.C. § 2246(3).
20 U.S.C. Sec. 6801 47 U.S.C. Sec. 254 47 U.S.C. Sec. 254(h)	**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.
18 U.S.C. Sec. 1460 18 U.S.C. Sec. 2256	**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.
3. Authority	Access to the District's networks and the Internet through school resources is a privilege, not a right. Inappropriate, unauthorized, and illegal use may result in the revocation of those privileges and appropriate disciplinary action. The network and the 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. 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, and the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Network users have no privacy expectation in the contents of their personal files or any of their use of

the District's network. The District reserves the right to log and monitor network 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 visual, graphic, text and any other form of obscene, child pornography, or other material that is harmful to minors, hateful, illegal, defamatory, harassing, violent and terroristic and any additional matter locally determined inappropriate material as a result of the District's local meeting or hearing before the public. 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 other lawful purpose.

Restrict or limit usage of lower priority network and computer uses when network and computing requirements exceed available capacity according to the following priorities:

1. Highest – uses that directly supports the education of the student.
2. Medium – uses that indirectly benefit the education of the student.
3. Lowest – uses that include reasonable and limited educationally-related interpersonal communications and, for staff, incidental personnel communications.
4. Forbidden – all activities in violation of this policy.

The District additionally reserves the right to:

1. Determine which network services will be provided through District resources.
2. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network, including e-mail.
3. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time and after notification to the user.
4. Log Internet and network use by students and staff.
5. Revoke user privileges, remove user accounts, and refer to legal authorities when violation of this and any other applicable District policies occurs or state and federal law is violated, including, but not limited to, those governing network use, copyright, security, discipline

	and vandalism of District resources and equipment. Responsibility 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, profane, pornographic, offensive, and illegal, can be accessed through the network. 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 privileges and disciplinary action as outlined in appropriate District policies. The District recognizes the importance of teaching acceptable use and online safety to students. The District shall educate all students about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and in cyberbullying awareness and response.
4. Delegation of Responsibility	The Director of Technology and Communications will serve as the coordinator to oversee the District system and will work with other regional or state organizations as necessary. In conjunction with the Director of Technology and Communications, the building principal will serve as the building-level coordinator for the District system, will approve building-level activities, ensure teachers receive proper training in the use of the system and the requirements of this policy, establish a system to ensure adequate supervision of students using the system, maintain executed user agreements, and be responsible for interpreting the District Acceptable Use Policy at the building level. The Director of Technology and Communications will establish a process for setting up individual and class accounts, set quotas for disk usage on the system, establish a retention schedule, and establish a District virus protection process. Unless otherwise denied for cause, student access to the Internet, e-mail, or other network 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 this resource. All users have the responsibility to respect the rights of all other users, both within the District network and throughout the Internet and to abide by the rules established by the District and its Internet service provider. 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. 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. 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 network.
5. Guidelines	<u>Access to the System</u> Network user accounts will be used only by the authorized owner of the account for its authorized purpose. An account will be made available according to a schedule developed by appropriate District authorities given the capability of District hardware. Accounts will be provided only to those individuals who meet the following requirements: 1. Have read the District Internet policy and indicate their agreement with its provisions by signing the signature page and returning it to the appropriate District authority. Students must have their parent/guardian sign the signature page indicating the parent's/guardian's agreement with the policy and their consent to allow the student to access and use the network. 2. Have successfully completed a learning experience, which will include, but not be limited to, instruction on network access, use, acceptable vs. unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities. This requirement shall apply to both students and District employees. Types of services included, but not limited to: 1. **District System.** The District's Acceptable Use Policy will govern all use of the District system. Student use of the system will also be governed by the relevant District policy. 2. **World Wide Web.** All District employees and students will have access to the Web through the District's networked computers. 3. **E-Mail.** District employees will be provided with an individual account. However, students may be assigned individual e-mail accounts for educational purposes.

4. **Guest Accounts.** Guests may receive an individual account with the approval of a District administrator if there is a specific, District-related purpose requiring such access. Use of the system by a guest must be specifically limited to the District-related purpose. An agreement will be required and parental signature will be required if the guest is a minor.

Parental Notification and Responsibility

The District will notify the parents/guardians about the District network and the policies governing its use. Parents/Guardians must sign an agreement to allow their student to have an individual network logon account.

The District will notify parents/guardians about the District's network and the policies governing its 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 system. Parents/Guardians are responsible for monitoring their children's use of the District's networks when they are accessing the system from home.

District Limitation of Liability

The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District system will be error-free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

Prohibitions

The use of the Internet computer network for illegal, inappropriate, unacceptable, or unethical purposes by students or employees is prohibited. All users of the network are strictly prohibited from engaging in the activities listed below. The District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the network.

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 to/for:

1. Non-work or nonschool related communications unless the employee's use comports with this policy's definition of incidental personal use.

2. Access indecent, obscene, pornographic, child pornographic or terroristic material.

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

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

5. Participate in discussion or news groups which cover inappropriate and/or objectionable topics or materials, including those which may be defamatory, inaccurate, obscene, profane, pornographic, offensive, terroristic and/or illegal.

6. Sending terroristic threats, hate mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.

7. Participate in unauthorized Internet Relay Chats, instant messaging communications and Internet voice communications (on-line; real-time conversations).

8. Facilitate any illegal activity.

9. Communicate through e-mail for non-educational purposes or activities, unless it is for an employee's incidental personal use as defined in this policy.

10. Commercial, for-profit, or business purposes (except where such activities are otherwise permitted or authorized under applicable District 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 District purchase of goods or supplies through the District system.
46 P.S. Sec. 148.1 et seq. 25 P.S. Sec. 3241 et seq.	11. Political lobbying, as defined by the Pennsylvania Lobbying Registration Act, as amended, and the Pennsylvania Election Code, as amended. District employees and students may use the system to communicate with their elected representatives and to express their opinion on political issues. 12. Advertising of any kind, unauthorized fundraising or unauthorized use of the District's name will not be permitted on the Internet or e-mail, or any other online service. 13. Anything that results in a copyright violation. 14. The illegal installation, distribution, reproduction or use of copyrighted software on District computers, or the copying of District software to unauthorized computer systems. 15. Intentionally infringing upon the intellectual property rights of others. 16. Use of the network to commit plagiarism. 17. Making available material or information the possession or distribution of which is illegal. 18. Unauthorized access, interference, possession, or distribution of confidential or private information. 19. Intentionally compromising the privacy or security of electronic information. 20. Posting personal web pages without administrative approval. <u>Access and Security Prohibitions</u> Users must immediately notify the Director of Technology and Communications if they have identified a possible security problem. The following activities related to access to the District's computer network 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 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 communication originally received from another person or computer with the intent to deceive.

6. Use of the District system 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 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 number of individuals or hosts. In other words, the user may not hack the network or others' computers, whether by spy ware 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 information, or completely take over a person's computer.

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

3. Unauthorized scanning of the 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 re-transmission of any computer or network services.

6. Connecting unauthorized hardware and devices to the 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 District computer hardware or software.

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

11. Negligence leading to damage of District electronic information, computing, or networking equipment.

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

Content Guidelines

Information electronically published on the District's network, including, but not limited to the District's World Wide Web pages shall be subject to the following guidelines:

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

2. Documents or videoconferences may not include information which indicates the physical location of a student at a given time other than attendance at a particular school or participation in school activities.

3. Documents or videoconferences may not contain objectionable material or point directly or indirectly to objectionable materials.

4. Documents must conform to District policies and guidelines, including the copyright policy.

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 system.

In the event there is an allegation that a student has violated the District's Acceptable Use Policy, the student will be provided with a written notice of the alleged violation and an opportunity to be heard in the manner set forth in the Student Disciplinary Code.

Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network. If the alleged violation also involves a violation of other provisions of the Student Disciplinary Code, the violation will be handled in accordance with the applicable provision of the Student Disciplinary Code.

Employee violations of this policy will be handled in accordance with District policy.

The District may terminate the account privileges of a guest user by providing notice to the user. Guest accounts not active for more than thirty (30) days may be removed, along with the user's files without notice to the user.

Search and Seizure

User violations of the District Acceptable Use Policy, the Student Disciplinary Code, 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.

District employees should be aware that their personal files very well may be discoverable and could be discoverable in the event of any form of litigation. Everything that District employees place in their personal files should be written as if a third party would review it.

The District reserves the right to monitor any electronic communications, including but not limited to Internet access, and e-mails. Students and employees should not have the 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 the District system. 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 copyright, 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' 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 – shrink-wrap, clickwrap and electronic software downloaded from the Internet.

District guidelines on plagiarism will govern use of material accessed through the District system. 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 the 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 sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site. 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.

District Web Site

District Web Site. The District will establish and maintain a Web site and will develop Web pages that will present information about the District. The Director of Technology and Communications or designee will be designated the Webmaster, responsible for maintaining the District Web site.

School Web Pages. Schools will establish and maintain Web pages that present information about the school or class activities. The building Instructional Assistant for Technology will be responsible for managing the school Web site.

Safety

To the extent possible, users of the network and Internet will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator.

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 spy ware, cookies, or use the network in any way to invade privacy. Additionally, the user may not disclose, use or disseminate personal information of other students or employees including, but not limited to, student's 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 home address, telephone numbers, school address, and work address.

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

Documents or videotapes may not include information which indicates the physical location of a student at a given time other than attendance at a particular school or participation in school activities.

Consequences for Inappropriate Use

Students and employees must be aware that violations of this policy or unlawful use of the computers, Internet or District networks may result in disciplinary actions.

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

General rules for behavior and communications apply when using the network and the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions may result from inappropriate use. For example, disciplinary action may be taken for inappropriate language or behavior in using the computers, District network or Internet services.

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

Violations as described in this policy may be reported to the appropriate legal authorities, whether the Internet service provider, local, state, or federal law enforcement. The District will cooperate fully with authorities in all such investigations.

Vandalism will result in cancellation of access to the network.