#4407

STUDENTS

Acceptable Use and Internet Safety Policy

The Board of Education of the Tuxedo Union Free School District(the District) is committed to the goals of improved student learning and effective teaching. The Board believes that access to computer networks, including the Internet and other technologies, can be an effective and valuable educational and research tool. The Board further believes that the computer network system, through software applications, online databases, bulletin boards and the Internet, and emerging features and uses of an electronic network, will significantly enhance student learning, as well as provide local, statewide, national and global communications opportunities for staff and students. Therefore, it is the policy of the Board to support and encourage the use of computers and computer-related technology in order to support open research and education in the District. The use of the computer network system for other purposes, including but not limited to for-profit or commercial activity, personal business or illegal activity is prohibited.

All users of the District's computer network system, including but not limited to electronic equipment, electronic mail and the Internet, must understand that use is a privilege, not a right, and that such use entails responsibility on the part of the user. Computer access will be provided by the District for each student and staff member who completes and submits the appropriate Acceptable Use Policy (AUP). In order to assure the integrity of the computer network system in the District, each account holder must agree to act responsibly and to comply with this Policy and its implementing Regulations. Therefore, prior to the establishment of a user account by the District, each student member and staff member must sign an AUP. In the case of students, the student's parent or guardian must also sign the AUP.

The Superintendent of Schools shall develop rules and regulations governing the use and security of the District's computer network system.

THE DISTRICT WEB PAGE

The District web site should promote and enhance educational opportunities and provide timely and appropriate information to the school district's community. The use of this District website will be consistent with the District's mission and goals and Board of Education policies.

All web pages residing on or pointing to a District-supported server or service are the property of the Tuxedo Union Free School District. Commercial use, use for the pursuit of personal or financial gain, advertising, soliciting, as well as use for any personal purpose are prohibited. The Superintendent of Schools and/or designee may suspend webpage access at any time if an individual fails to adhere to the protocol requirements stated herein. Each teacher/staff is responsible for the content posted on his/her webpage hosted on the District-supported servers/services and will follow all District procedures. Teachers and District employee web pages may link only to sites that are of educational significance and sites relating to the curriculum and activities of the District. In addition, all links must comply with State and Federal law, including the Children's Internet Protection Act (CIPA).

The Superintendent will designate staff member(s) who will be responsible for monitoring the accuracy and consistency of webpage content. This staff member(s) has the right to view, edit, modify, or delete without notice any material deemed inappropriate. Access to administrative areas is limited to authorized personnel only.

INTERNET SAFETY

Internet access is provided with the understanding that the District cannot control the content available on the Internet. While the vast majority of sites available provide a wealth of useful information to staff and students, some sites may contain information that is inaccurate, offensive, defamatory or otherwise inappropriate for students. The District does not condone or permit the use of such materials in the school environment and makes good faith efforts to limit access by students to such inappropriate materials.[1]

The District, in accordance with the Children's Internet Protection Act (CIPA), requires all District computers with access to the Internet to be equipped with filtering or blocking technology that blocks access by adults to visual depictions that are obscene[2] or child pornography[3] and by minors to visual depictions that are obscene, child pornography or harmful to minors.[4] All current and new computers will have internet access through a filtering

---

[1]*Inappropriate materials* means any material that is obscene, child pornography or harmful to minors.

[2]*Obscene* means any material or performance when, considered as a whole, predominately appeals to a prurient interest in sex; or that depicts or describes in a patently offensive manner actual or simulated sexual acts, sexual contact, nudity, sadism, masochism, excretion, or a lewd exhibition of the genitals and that lacks serious literary, artistic, political, or scientific value.

[3]*Child Pornography* means 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 the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) 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.

[4]*Harmful to minors* means any picture, image, graphic file or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion; (b) 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 contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (c) taken as a whole, lacks serious literary, artistic, political or scientific value as to minors.

or blocking mechanism. This shall be documented by the District in accordance with the CIPA. The District, however, does not guarantee that students will be prevented from accessing all inappropriate locations and proper supervision will be provided to students in school to further ensure appropriate usage. Under certain supervised circumstances, authorized personnel may override the filtering/blocking technology for a limited period of time to assist students/staff with special projects or research. District guidelines will be developed to implement this component of the policy.

All use of the District's computer network, including access to the Internet is a privilege and not a right, and that any such use entails responsibility. Parents, staff members and students must be aware that is the responsibility of the user to monitor his/her own access and to use sound judgment. However, the District, through its staff members, technology and systems reviews, shall monitor online activities of students and staff while in school, including but not limited to use of e-mail, chat rooms and other forms of direct electronic communication, "hacking" and other unlawful activities by minors and access to materials harmful to minors.

The District shall also provide age appropriate instruction to students regarding appropriate online behavior. This instruction shall include but not be limited to**:** positive interactions with others online, including on social networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and how to recognize and respond to cyberbullying and other threats. Such instruction will be provided even if the District prohibits students from accessing social networking sites and chat rooms on District technology.

PRIVACY

Users acknowledge that the network administrator may periodically need to review on-line activities in the course of performing routine maintenance of the system. Users further acknowledge that if there is reasonable suspicion of a user having violated this Policy or its implementing regulations, or any applicable law, the network administrator and/or appropriate

school official may require access to his/her files, including private correspondence and private files, to review on-line activities. Any administrator reviewing such files in accordance with this Policy shall not be subject to any claims arising out of such review.

The Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet. The Superintendent or designee shall establish and implement procedures that enforce these restrictions.

DISCLAIMER OF LIABILITY

The Tuxedo Union Free School District disclaims all liability for the content of material that a student may access on the Internet, for any damages suffered in the course of or a result of the student's Internet use, and for any other consequences of a student's Internet use.

The District makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the District assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the District's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The District will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or the errors or omissions of any user. The District also will not be responsible for unauthorized financial obligations resulting from the use of or access to the District's computer network or the Internet.

Further, even though the District may use technical or manual means to regulate access and information as required by the Children's Internet Protection Act (CIPA), these methods do not provide a foolproof means of enforcing the provisions of the District policy and regulation.

SANCTIONS

All users of the District's computer network and equipment are required to comply with the District's policy and regulations governing the District's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

Approved: 05/23/96
Revised: 08/24/10, 7/2/12

#4407R

SUPERINTENDENT'S REGULATION FOR THE USE AND SECURITY OF THE DISTRICT'S COMPUTER NETWORK SYSTEM

The following rules and regulations govern the use of the District's computer network system, the District website and access to the Internet:

I. ADMINISTRATION

- The Superintendent of Schools shall identify a Director of Technology who will be responsible to oversee the District's computer network and the technology function.
- The Director of Technology shall oversee the monitoring and examination of all network activities, as appropriate, to ensure proper use of the system.
- The Director of Technology shall be responsible for disseminating and interpreting District policy and regulations governing use of the District's network at the district and the building level with all network users.
- The Director of Technology shall coordinate employee training for proper use of the network and will ensure that staff supervising students using the District's network provide similar training to their students, including providing copies of District policy and regulations governing use of the District's network.
- The Director of Technology shall ensure that virus protection is functional across the entire network, including servers, workstations and software.
- All student agreements to abide by District policy and regulations and parental consent forms shall be kept on file in the main office of each school building.
- All staff agreements to abide by District policy and regulations shall be kept on file in the business office.

II. INTERNET ACCESS

In compliance with the Children's Internet Protection Act (CIPA), the District filters all access to through District managed equipment.

- Students will be provided access during the instructional day.
- Students will be provided with individual District network accounts, with signed parent/guardian permission.
- Students may access the Internet for information and related resources.
- Students may participate in online learning activities under the supervision of the classroom teacher or other adult supervisor.
- A staff member will be required to monitor these activities.

III. WEBPAGE SECURITY AND CONFIDENTIALITY

The privacy of students and employees will be respected

- Student first names or initials only are to be published

- A child's or employee's name should never be linked with a photo
- Contact information for an employee will be restricted to school address, work phone numbers and District e-mail address
- Publication of personal address, phone numbers, or email addresses is prohibited
- Links to personal web pages and sites that contain inappropriate material are prohibited

IV. ACCEPTABLE USE AND CONDUCT

- Access to the District's computer network is provided solely for educational purposes and research consistent with the District's mission and goals.
- Use of the District's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege as per the Code of Conduct.
- Each individual in whose name an access account is issued is responsible at all times for its proper use.
- All network users will be issued a login name and password. Passwords must be changed in accordance with the current District practice..
- All network users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive or sexual language or images, vulgarities and swear words are all inappropriate.
- Network users identifying a security problem on the District's network must notify the appropriate teacher, administrator, IT professional, or Director of Technology. Under no circumstance should the user demonstrate the problem to anyone other than to the District official or employee being notified.
- Any network user identified as a security risk or having a history of violations of District computer use guidelines may be denied access to the District's network.

V. PROHIBITED ACTIVITY AND USES

The following is a list of prohibited activity concerning use of the District's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising.
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the District computer network (plagiarism).
- Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Using another user's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.

- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the District's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software on the District's computers and/or network.
- Using District computing resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Sending unsolicited email messages, including the sending of "junk mail" or other advertising materials to individuals who did not specifically request such materials (email spam). This includes creating or forwarding of "chain letters", "Ponzi" or other "pyramid" schemes of any type.

AGREEMENT BETWEEN THE TUXEDO UNION FREE SCHOOL DISTRICT AND NETWORK/INTERNET ACCOUNT HOLDERS.

I, the undersigned, have read and agree to the terms and conditions set forth in this Acceptable Use Policy (Policy #4407 – dated 08/24/10). I further understand that any violation of the regulations may constitute a criminal offense. Should I commit a violation, my access privileges may be revoked, school disciplinary action and/or the appropriate legal action may be taken.

Account Holder (Print) _____

Account Holder (Signature) _____

Date: _____

If the account holder is a student, then parent signature is required.

I, the parent/legal guardian of the above, understand the contents of this document and agree to be bound by its terms and conditions.

Parent (Print) _____

Parent (Signature) _____

Date: _____

Form Approved date: 05/03/96
Revised: 08/24/10, 7/2/12