Tuckahoe Union Free School District
RESPONSIBLE COMPUTER USE POLICY
Computer, District Issued Technology and Internet Use

The Tuckahoe Union Free School District is committed to optimizing student learning and teaching and considers student access to technology, including the Internet, to be an essential educational and research tool. A technologically rich curriculum promotes active, higher order, and collaborative learning. It is essential for today's learner to have access to technological resources in support of higher education. To support such endeavors, the district has engaged in a technology for all initiative, and self-monitoring and correction by students and staff is an expectation for the responsible use of these resources.

Each user--student or staff--is responsible for his/her actions while using district resources, including but not limited to bandwidth (a finite resource), student or district devices, software, and online resources.

The District has developed protocol governing the use and security of the district's computer network and District-owned technology. All users of the district's computer network and equipment shall comply with this policy. Use of the District's technology and network is a privilege, not a right. All users of the district's computer network and equipment are required to comply with the district's policy 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.

RULES GOVERNING RESPONSIBLE COMPUTER USE

The following rules govern the use of technology on the district's computer network system and access to the Internet. It is each individual's responsibility to use our district's technology resources in a responsible manner.

In enforcing this policy, the Superintendent's designee will oversee the District's network. The coordinator shall:

- Monitor network activities, as appropriate, to ensure proper use of the system;
- Disseminate and interpret District policy governing use of the District's network at the building level with network users;
- Provide employee training regarding the proper use of the network;
- Distribute this policy on an annual basis to students and staff;
- Ensure disks and software loaded onto the computer network are free of computer viruses; and

- Maintain signed agreements to abide by this policy.

INTERNET ACCESS AND USE

- Students and Staff may access the internet for education purposes only.
- During the school day, students access the internet solely through the district's wireless connections. Students should not connect via cellular carrier (i.e. 3G or 4G) or their own personal Internet providers (i.e. Optonline hotspots) as these are not filtered by the district.
- Students and Staff will be provided with password protected individual accounts and are responsible for all activity on their account. Sharing of passwords and/or accounts shall not be permitted.
- Students and Staff may use the World Wide Web and Internet for items related to the district's instructional goals. They are encouraged to take advantage of all available resources including multimedia and streaming resources.
- Students may only participate in district sponsored social networks (i.e. Google Communities, Edmodo) and those specifically provided by or approved by the teacher.
- Students and Staff must refrain from use of the internet for personal reasons.
- Students and Staff may construct their own web pages, apps, or other digital resources using district technology resources if these are created and utilized in connection with the district's instructional goals and comply with the district's responsible use policy.
- Students and Staff will have an individual e-mail address assigned by the district. The content of any email sent or received from a District account shall not be considered private and may be reviewed by teachers, administrators, and other authorized parties at any time without prior notification. All email shall be regarded as having the same status as a postcard. Despite various precautions, email is not an appropriate medium for the transmission of sensitive or confidential information. When in doubt, alternative methods of communication should be employed or advice sought.
- Students and Staff must adhere to the policies governing confidentiality of student and staff information (i.e. personal, academic, personnel, health).
- Staff must safeguard their passwords. Staff passwords often give access to confidential information (i.e. student management system, financial system, IEP system) and keeping them secure is a necessary responsible use of our resources.
- Network users identifying a security problem on the district's network are expected to notify the appropriate teacher, administrator or the District. Under no circumstance should the user demonstrate the problem to anyone other than to the district official or employee being notified, as this would be an irresponsible use of district resources.

ETIQUETTE

- Be polite. Do not write or send abusive, harassing, obscene, or threatening messages or notes.
- Use appropriate language. Do not swear or use vulgar language.

- Do not give personal information (your or another's) to others. This includes, but is not limited to, personal user ID, name, address, phone number, password.
- Do not use the network in such a way that it disrupts the use of the network by other users or intentionally waste limited computer resources.

BRING YOUR OWN TECHNOLOGY

The District offers "Bring Your Own Technology" to staff as a courtesy, and assumes no responsibility for any device that is damaged, lost, or stolen. Additionally, the district cannot provide support for personal devices. In the event staff BYOT to school, employees must utilize the District's wireless Internet connection and comply with all applicable provisions of the district's responsible computer use policy. Staff members will be required to oversee the use of technologies that they assign.

ACCEPTABLE USE

- Access to the district's computer network is provided for educational purposes and research consistent with the district's mission and goals.
- 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 periodically.
- Only those network users who have properly registered their device with the computer network coordinator, or who have been issued a district-owned device, may access the district's system from off-site (e.g., from home).
- 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 or computer network coordinator. 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.

PROHIBITED ACTIVITY/USE

- 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.
- 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.
- Using the network for sending and/or receiving personal messages.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the district's computers and/or network without the permission of the appropriate district official or employee.
- 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.
- Wastefully using finite district resources.
- Changing or exceeding resource quotas as set by the district without the permission of the appropriate district official or computer network coordinator.
- 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.
- 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.

SUPERVISION AND MONITORING:

The Tuckahoe Union Free School District reserves the right to monitor District issued technology devices, in addition to users' online activities and to access, review, copy and store or delete any electronic communication or files and disclose them to others as it deems necessary. Users should have no expectation of privacy regarding their use of District property, network and/or Internet access or files, including e-mail. School and network administrators and their authorized employees shall frequently monitor the use of information technology resources to help ensure that uses are secure and in conformity with this policy and may deny, revoke, or suspend specific user accounts and/or access if found to be in violation.

DISCLAIMER:

The Tuckahoe Union Free School District makes no guarantee about the quality of the services provided and is not responsible for any claims, losses, damages, costs or other obligations arising from use of the network or accounts. Any additional charges a user accrues due to the use of the District's network are to be borne by the user. The District also denies any responsibility for the accuracy or quality of the information obtained through user access. Any statement, accessible on the computer network or the Internet, is understood to be the author's individual point of view and not that of the Tuckahoe Union Free School District, its affiliates, or employees. Accordingly, anonymity is NOT allowed. As an educational institution, we believe that individuals must take responsibility for their actions and words.

The Tuckahoe Union Free School District makes no warranties of any kind, either expressed or implied, for the internet access it is providing. The school is not responsible for:

1. Any damages users suffer, including, but not limited to, loss of data resulting from delays or interruptions in service;
2. The accuracy, nature or quality of information stored on school diskettes, hard drives or servers or gathered through school-provided Internet access;
3. Personal property used to access school computers or networks or for school-provided Internet access; or
4. Unauthorized financial obligations resulting from school-provided access to the Internet.

The individual in whose name a system account is issued will be responsible at all times for its proper use. Thus, users have full responsibility for the use of their account. All violations of this policy will be treated as the sole responsibility of the owner of the account. Any violation of this policy must be reported to school administrators.

I have read the 'District Acceptable Use Policy' and I agree to follow the rules contained therein. I understand that if I violate the rules, access to the Internet and/or District can be terminated and I may face other disciplinary measures. In the event I am issued a District owned device, I understand my misuse of the computer network or the device may result in revocation of privileges.

Date: _____ Grade/Teacher:_____

Student's Name: _____ Parent or Guardian's Name: _____

Student's Signature: _____ Parent or Guardian's Signature: _____