

Tantasqua/Union 61 Acceptable Electronic Network Use Policy

Tantasqua/Union 61 is providing staff and students (users) access to the district's electronic network. This network includes Internet access, computer services, videoconferencing, computer equipment and related equipment for educational purposes. The purpose of this network is to assist in preparing users for success in life and work in the 21st century by providing them with electronic access to a wide range of information and the ability to communicate with people throughout the world. This document contains the rules and procedures for users' acceptable use of the Tantasqua/Union 61 electronic network.

- The Tantasqua/Union 61 electronic network has been established for a limited educational purpose. The term "educational purpose" includes classroom activities, classroom assignments or career development.
- The Tantasqua/Union 61 electronic network has not been established as a public access service or a public forum. Tantasqua/Union 61 has the right to place reasonable restrictions on material that is accessed or posted throughout the network.
- Parent/guardian permission is required for all users under the age of 18. Access is a privilege — not a right.
- The district is not responsible for the actions of users who violate the agreement beyond the clarification of its terms.
- The district reserves the right to monitor all activity on this electronic network. Users will indemnify the district for any damage that is caused by users' inappropriate use of the network.
- Users are expected to follow the same rules, good manners and common sense guidelines that are used with other daily school activities as well as the law in the use of the Tantasqua/Union 61 electronic network.

General Unacceptable Behavior

While utilizing any portion of the Tantasqua/Union 61 electronic network, users will not use the district equipment, network, or credentials to send, post or receive electronic messages, or engage in behaviors that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal. Unacceptable behaviors include, but are not limited to, the following:

- Posting information that, if acted upon, could cause damage or danger of disruption.
- Engaging in personal attacks, including prejudicial or discriminatory attacks.
- Bullying or Cyberbullying
- Harassing another person. Harassment is defined as persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending messages, they must stop.
- Knowingly or recklessly posting false or defamatory information about a person or organization.
- Using criminal speech or speech in the course of committing a crime such as threats to the president, instructions on breaking into computer networks, child pornography, drug dealing, purchase of alcohol, gang activities, threats to an individual, etc.
- Using speech that is inappropriate in an educational setting or violates district rules.
- Abusing network resources such as sending chain letters or "spamming."
- Displaying, accessing or sending offensive messages or pictures.
- Using the Tantasqua/Union 61 electronic network for commercial purposes. Users will not offer, provide, or purchase products or services through this network.

- Using the Tantasqua/Union 61 electronic network for political lobbying and/or campaigning.
- Users may only use the system to communicate with elected representatives on issues related to a class assignment or project and to communicate with elected officials only for school/district related activities and/or issues.
- Attempting to access non-instructional district systems, such as student information systems or business systems.
- Using any wired or wireless network (including third party internet service providers) with equipment brought from home. Example: The use of a home computer on the network or accessing the internet from any device not owned by the district is not allowed.
- Using district equipment, network, or credentials to threaten employees, or cause a disruption to the educational program.

E-Mail

- E-mail for student users in the elementary and junior high grades is not provided.
- Users will not repost a message that was sent to them privately without the permission of the person who sent them the message.
- Users will not post private information about another person.

World Wide Web

- Elementary School Level - Access to information for student users on the Web will generally be limited to prescreened sites that are closely supervised by the teacher.
- Junior and Senior High School Level - Access to information for student users on the Web will generally be provided through prescreened sites and in a manner prescribed by their school.

Telnet and FTP

- Telnet and FTP services will not be available to users.

Message Board/Usenet Groups

- The district will provide access to selected newsgroups that relate to subjects appropriate for educational use. Messages posted locally that are in violation of this policy will be removed. The district reserves the right to immediately terminate an account of a user who misuses the message boards or Usenet groups.

Real-time, Interactive Communication Areas

- Users will not use chat or instant messaging without the permission of the Principal or Superintendent.

Software and Files

- Software is available to users to be used as an educational resource. No user may install, upload, or download software without permission from the district technology department.
- A user's account may be limited or terminated if a user intentionally misuses software on any district-owned equipment.
- Files stored on the network are treated in the same manner as other school storage areas. Routine maintenance and monitoring of the Tantasqua/Union 61 electronic network may lead to discovery that a user has violated this policy or the law. Users should not expect that files stored on district servers are private.

Web Sites

- Elementary and Junior High Level - Group pictures without identification of individual student users are permitted. Student work may be posted with either student first name only or other school-developed identifier (such as an alias or number) upon notice to parents.
- Senior High School Level - Students may be identified by their full name with parental approval. Group or individual pictures of users with student identification are permitted with parental approval. Parents may elect to have their child assigned to the elementary/junior high level of use.
- Material placed on user Web pages are expected to meet academic standards of proper spelling, grammar and accuracy of information.
- Material (graphics, text, sound, etc.) that is the ownership of someone other than the user may not be used on Web sites unless formal permission has been obtained.

Personal Safety

- Users will not share personal contact information about themselves or other people. Personal contact information includes address, telephone, school address, or work address.
- Elementary and junior high student users will not disclose their full name or any other personal contact information for any purpose.
- High school student users will not disclose personal contact information, except to education institutes for educational purposes, companies or other entities for career development purposes, or without specific building administrative approval.
- Users will not agree to meet with someone they have met online.
- Users will promptly disclose to a teacher or other building administrator any message received that is inappropriate or makes the user feel uncomfortable

System Security

- Users are responsible for their individual accounts and should take all reasonable precautions to prevent others from being able to use them. Under no conditions should users provide their password to another person.
- Users must immediately notify a teacher or the system administrator if they have identified a possible security problem. Users should not go looking for security problems, because this may be construed as an illegal attempt to gain access.
- Users will not attempt to gain unauthorized access to any portion of the Tantasqua/Union 61 electronic network. This includes attempting to log in through another person's account or access another person's folders, work, or files. These actions are illegal, even if only for the purposes of "browsing".
- Users will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means. These actions are illegal.
- Users will not attempt to access Web sites blocked by district policy, including the use of proxy services, software, or Web sites.
- Users will not use sniffing or remote access technology to monitor the network or other user's activity.

Technology Hardware

- Hardware and peripherals are provided as tools for educational purposes. Users are not permitted to relocate hardware (except for portable devices), install peripherals or modify settings to equipment without the consent of the district technology department.

Vandalism

- Any malicious attempt to harm or destroy data, the network, other network components connected to the network backbone, hardware or software will result in cancellation of network privileges. Disciplinary measures in compliance with the district's discipline code and policies will be enforced.

Plagiarism and Copyright Infringement

- Users will not plagiarize works found on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were the users'.
- District policies on copyright will govern the use of material accessed and used through the district system.
- Copyrighted material will not be placed on any system without the author's permission. Permission may be specified in the document, on the system, or must be obtained directly from the author.

Videoconference

- Videoconferencing is a way that users can communicate with other users, speakers, museums, etc. from other parts of the country and the world. With videoconferencing equipment, users can see, hear, and speak with other users, speakers, museum personnel, etc. in real-time.
- Videoconference sessions may be videotaped by district personnel or by a participating school involved in the exchange in order to share the experience within ours or their building or district.
- Users' voices, physical presence, and participation in the videoconference are transmitted to participating sites during each session. Rules and procedures relative to acceptable use and behavior by users apply during all videoconference sessions.

User Rights

- Users' right to free speech applies to communication on the Internet. The Tantasqua/Union 61 electronic network is considered a limited forum, similar to the school newspaper, and therefore the district may restrict a student's speech for valid educational reasons. The district will not restrict a student's speech on the basis of a disagreement with the opinions that are being expressed.
- An individual search will be conducted if there is reasonable suspicion that a user has violated this policy or the law. The investigation will be reasonable and related to the suspected violation.

Due Process

- The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the district network.
- In the event there is an allegation that a user has violated the district acceptable use regulation and policy, the user will be provided with a written notice of the alleged violation. An opportunity will be provided to present an explanation before a neutral administrator (or student will be provided with notice and an opportunity to be heard in the manner set forth in the disciplinary code).
- Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the user in gaining the self-discipline necessary to behave appropriately on an electronic network. Violations of the acceptable use regulation and policy may result in a loss of access as well as other disciplinary or legal action.

- If the violation also involves a violation of other provisions of other school rules, it will be handled in a manner described in the school rules. Additional restrictions may be placed on a student's use of his/her network account.

Limitation of Liability

- The district makes no guarantee that the functions or the services provided by or through the district network will be error-free or without defect. The district will not be responsible for any damage suffered, 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 network. The district will not be responsible for financial obligations arising through the unauthorized use of the network.

Violations of this Acceptable Use Policy

Violations of this policy may result in loss of access as well as other disciplinary or legal action. Users' violation of this policy shall be subject to the consequences as indicated within this policy as well as other appropriate discipline, which includes but is not limited to:

- Use of district network only under direct supervision
- Suspension of network privileges
- Revocation of network privileges
- Suspension of computer privileges
- Suspension from school
- Expulsion from school and/or
- Legal action and prosecution by the authorities

The particular consequences for violations of this policy shall be determined by the school administrators. The superintendent or designee shall determine when school expulsion and/or legal action or actions by the authorities are the appropriate course of action.

TRSD Adoption:	December 18, 2007
Brimfield Adoption:	January 22, 2008
Brookfield Adoption:	February 12, 2008
Holland Adoption:	February 14, 2008
Sturbridge Adoption:	January 3, 2008
Wales Adoption:	June 18, 2008
Amended First Reading:	November 16, 2010
Amended Second Reading:	December 21, 2010
Amended Adoption:	December 21, 2010

Cross References JICFB-1, Bullying Prevention and Intervention