No. 815-AR

TUNKHANNOCK AREA
SCHOOL DISTRICT

ADMINISTRATIVE
REGULATION

815-AR. INTERNET USE FOR STUDENTS

It is impossible to control access to all materials available through the Internet, and an industrious user may discover controversial information. Therefore, students will browse the Internet in supervised settings, and we require parent/guardian permission for student World Wide Web access. All computer users must act in a responsible, ethical, and legal manner as they use this resource.

The smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. We provide the guidelines here so that you are aware of the responsibilities you are about to acquire. This requires efficient, ethical, and legal utilization of the network resources.

The signatures on the Internet and Computer Access Permission Form is (are) binding and indicate(s) the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

Acceptable Use

The purpose of the Internet is to provide a resource with a limited-educational purpose. The district expects the same behavior on the Internet as what is required in class, in any area in the school, on any school property, or at any school function. This includes but is not limited to:

1. Use language that is considered appropriate.

2. Be polite.

3. Share information beneficial and appropriate to the educational purpose.

4. Conform to copyright laws.

5. Use the network in ways that will not interfere with others' use of the network.

The following are not acceptable nor permitted. Violators may be subject to the Student Code of Conduct, the legal authorities or both. The list is noninclusive:

1. Accessing or attempting to access adult sites, hate sites, sites that promote violence, or sites that promote illegal activities.

2. Chat rooms or any other form of direct electronic communications, (i.e., Instant Message Services) or sites for anything other than an educational purpose (i.e., no games or entertainment).

3. Accessing or attempting to access commercial sites, including those offering products or services. The user shall be held accountable and responsible for any and all costs or damages resulting from unacceptable activities.

4. Accessing or attempting to access information regarding network or system security.

5. **Plagiarism -** Using or attempting to use ideas or words of others as your own.

6. Accessing or attempting to access inappropriate material or material potentially harmful to minors.

   Inappropriate material includes, but is not limited to:

   a. Criminal speech and speech in the course of committing a crime, terroristic threats, instructions on breaking into computer systems, child pornography, drug dealing, purchase of alcohol, gang activities.

   b. Speech that is inappropriate in an educational setting or violates district rules necessary to maintain a quality educational environment.

   c. Inappropriate language, including obscene, profane, lewd, vulgar, rude, disrespectful, threatening, or inflammatory language; harassment; personal attacks, including prejudicial or discriminatory attacks; and false or defamatory material about a person or organization.

   d. Dangerous information that if acted upon could cause damage or present a danger or disruption.

   e. Violations of privacy that reveal personal information about others.

   f. Abuse of resources such as chain letters, spamming, and inappropriate use of district group distribution lists.

   g. Copyright infringement or plagiarism.

   h. Violations of personal safety, such as a student revealing personal contact information about him/herself or engaging in communication that could place the student in personal danger.

   Potentially harmful includes, but is not limited to any picture, image, graphic image 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 bodily functions.

   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 body or body parts.

c. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Conduct

All Board policies regarding student conduct extend to student conduct on the Internet. Computer systems and data on the Tunkhannock network and the Internet are the property of others. Attempts to break into other computer systems or unauthorized access is unauthorized use of school property and is subject to disciplinary actions defined in Board policy and student handbooks.

Network Etiquette

All users are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

1. Be polite. Do not get abusive in your messages to others.

2. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language. Do not engage in activities which are prohibited under state or federal law.

3. Do not reveal your personal address or phone numbers of other students or colleagues.

4. The system providers have access to all mail and the e-mail may be monitored. Messages relating to or in support of illegal activities will be reported to the administration for appropriate disposition and may result in loss of user privileges. E-mail may be used during the school day for school-related projects only. When giving out user names, only first names should be used. Private messaging and the use of private mail accounts for nonschool-related purposes are prohibited.

5. Do not use the network in such a way that you would disrupt the use of the network by others.

Security

1. Security on any computer system is a high priority. Users must never allow others to use their password and it is their responsibility to protect their password.

2. If you see a security problem on the Internet or any computer system, it is the responsibility of the user to report it and not to show or demonstrate it to others.

3. Do not use other individual’s accounts without written permission.

4. Attempts to log on to the Internet as a system administrator will result in cancellation of usage.

5. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet or computers by the administration of the district.

Vandalism And Harassment

1. Vandalism and harassment may result in cancellation of user privileges.

2. Students may have privileges revoked if they go into computer systems and change any configurations of the system.

3. **Harassment** is defined as the persistent annoyance of another user, or the interference of another user's work. Harassment includes, but is not limited to, sending of unwanted mail or misuse of user groups on the Internet.

Procedures For Use

1. Students must always have permission from a member of the faculty before using the Internet or any computer system. They must follow written and oral instructions.

2. Students must follow the procedures given to them by the faculty member.

3. All users have the same rights to use the equipment. Therefore, users shall not play games or use the computer resources for other nonacademic activities. Users shall not waste or take supplies that are provided by the district.

Encounter Of Controversial Material

Users may encounter material which is controversial and which users, parents/guardians, teachers or administrators may consider inappropriate or offensive. The district shall provide a firewall to try to prevent controversial materials on the Internet. However, on a global network it is impossible to control effectively the content of data. An industrious user may discover controversial material. Any decision by the administration to restrict access to the Internet material shall not be deemed to impose any duty on administration to regulate the content of material on the Internet.

Penalties For Improper Use

Any user violating these rules, applicable state and federal laws or posted classroom and district rules may be subjected to loss of all Internet and computer privileges and any other district and/or legal system/authorities disciplinary options.

Responsibilities Of Student In Their Use Of Internet Access

1. Students shall notify a teacher or a system administrator of any violations of this administrative regulation taking place by other Tunkhannock students or outside parties. This may be done anonymously.

2. You may not give your password to anyone.

3. You may not use or play games via the network unless it is part of a class assignment or project.

4. You may not use or alter anyone else's Internet account.

5. You may not offer Internet access to any individual via your Tunkhannock account.

6. You may not download or create a computer virus.

7. You may not destroy another person's data.

8. You may not monopolize the resources of Tunkhannock Internet. This includes things such as running large jobs during the day, sending massive amounts of e-mail to Tunkhannock users, or using system resources for games.

9. You are not permitted to get from or put onto the network any copyrighted material (including software), or threatening or obscene material.

10. Purposefully annoying other Internet users, on or off the Tunkhannock system, is prohibited. This includes things as continuous talk requests.

11. Illegal activities may not be conducted via the network.

12. All communication and information accessible via the network should be assumed to be private property even though privacy cannot be guaranteed.

13. Before any file is downloaded, permission must be obtained from the monitoring teacher. The intent of this regulation item is to limit the downloading of music, movies, games, etc.