

**Policies and Procedures for Computer
and Internet Use**

Internet Protection Policy

Electronic Communication Policy

Tioga Central School District

Tioga Center , New York 13845

August 2006

Special acknowledgement is given to:

Hofstra University

Nassau School Library

SCT BOCES

Hogan & Sarsynski, LLP

in their assistance in the creation of this document.

A PHILOSOPHY REGARDING USE OF ELECTRONIC COMMUNICATION

The Tioga Central School District recognizes that electronic communication is now a very important aspect of the educational process. However, it also recognizes that electronic communication should not replace the human aspect of one-to-one discussion and information exchange.

Philosophy of Computer Use

The same morality and ethical behavior that applies in the non-computing environment applies in the computing environment. Computer use is a public facility and, as such, requires the exercise of common sense, courtesy, and rules to maximize the benefit for all. You need to be aware of the impact of your computer and internet use on others.

Computer use and communication paths are analogous to a public road system. Just as there are rules of the road, there are rules of computing system use where the computer becomes common ground for all users. Beyond public roads come private roads and driveways – analogous to user accounts and files.

In traversing a system, there are responsibilities, both internal and external (use of private and public roads), that must be accepted. Failure to heed basic rules or guidelines can result in damage to property or injury to others. This misuse can be in the form of physical property damage or bodily harm or of computer file or system damage and the loss of hours of hard work. Both environments have standards, explicitly stated or implied, and each are governed by laws, rules, or social customs. These standards form a framework of accepted behavior, aimed at benefiting all involved.

The continued use of computing resources in a relatively free and open way depends upon how well one “shares the road,” that is, complies with the Code of Conduct. The spirit and the letter of the rules are critical. Only through cooperation with

other users can we all achieve our academic and administrative objectives through computer use.

Since this policies and procedures document is prepared specifically for educational computing and electronic communication, these standards and guidelines are explicitly written to protect the student body and provide a safe computing and communications environment in an educational setting.

Code of Conduct

Rules of computer conduct include, but are not limited to, the list which follows. Interpretation of the rules of conduct and issues regarding ownership of developed works and copyrights of commercial products should be directed to the Superintendent of Schools

Those who abuse the privilege of using Tioga Central's computing resources may lose computing privileges and may be subject to criminal prosecution. The rules of conduct for computer use are as follows:

1. Follow all procedures for computer, network, internet, and communication use, including e-mail, within this document: **Policies and Procedures for Computer and Internet Use at Tioga Central, Internet Protection Policy, and Electronic Communication Policy.**

2. Remember that Tioga Central's computer labs are public property and should be treated with care and respect. Please leave the facilities in the same condition in which you found them. Should you discover maintenance problems or the room(s) left in an unacceptable condition, please report the situation to your Building Principal and Tioga Central's Computer Coordinator.

3. Scheduling Procedures:

Middle School and Elementary Schools:

Sign up on the permanent schedule to reserve a set time each week for your class.

OR

Sign up for lab use at an available time slot not permanently scheduled.

OR

When necessary, discuss a selected time with the teacher who has already reserved that time slot in order to work out a compromise.

High School:

Reserve computer lab at least **one week in advance** by signing your name and class periods needed on the master schedule located in the computer lab. For those cases when pre-planning was impossible, contact the high school computer support staff **prior** to just sending your students to the computer lab to ensure that the room is available and supervised.

4. All teachers must accompany their students to the computer labs and supervise the class while in the lab and on the way to and from the classroom.
5. Should you have any specific software or hardware set-up requests, please make these known to the computer support staff at least **two weeks** in advance. It is recommended that teacher planning allow for computer time sign-up at least one week in advance of required use of the computer lab(s).
6. Be flexible, try to plan ahead, and communicate to avoid conflicts. When necessary, compromise.
7. **NO FOOD OR DRINK IS ALLOWED IN THE COMPUTER LABS.** This rule applies to **BOTH STUDENTS AND STAFF** and to all computer locations throughout the Tioga Central School District. Please be mindful of food and/or drink near computers within your classroom as well.
8. Use only Tioga Central licensed and installed software.
9. Use only Tioga Central installed hardware.
10. Do not install any of your own software or hardware without checking with the Tioga Central Computer Coordinator. This person will assist you in making the decision to install a particular piece as well as in performing the installation for you.
11. Leave the room as you found it: neat, clean, and orderly. There will be no guarantees that material left in the computer lab(s) will remain there indefinitely as the labs are cleaned each day.
12. When confronted with a computer, disk, printer, or network problem, please seek assistance by submitting a work order to Tioga Central's Computer Coordinator. The problem will be addressed as soon as possible.

13. Please report any observed misuse of the computer lab(s) or computer equipment anywhere in the School District to Tioga Central's Computer Coordinator and to the Building Principal where the incident occurred.

14. Please report any chronic problems or performance irregularity in computer equipment and software dependability to Tioga Central's Computer Coordinator so that the problem can be tracked and corrected. Again, please describe the problem on the District's standard work order and submit this form to the Computer Coordinator.

15. Tioga Central's Computer Coordinator will provide you and your students with appropriate network folder(s) or disks to use in computers at Tioga Central. These disks must remain in the computer lab(s) or under the care and supervision of the classroom teacher. **An alternative to saving work on disk is to save to the network drive assigned to each individual within Tioga Central's network.** Any portable device used for saving a person's work (such as the "key chain" type portable devices) must be scanned for viruses before use in Tioga Central's network.

16. You may not attempt to modify in any way a program diskette, which the School District supplies for any types of use at its sites. All diskettes remain the property of the School District and must be stored in the appropriate computer lab or with the appropriate classroom teacher.

17. You may not use a computer ID that was not assigned to you by the Tioga Central School District. You may not try in anyway to obtain a password for another's computer ID. You may not attempt to disguise the identity of the account or machine you are using. **Each individual within Tioga Central's school community will have an assigned user name and password for the purpose of logging into Tioga's network and for access to his or her network drive, printing, and network software.**

18. You may not present false identification or misleading information to gain access to computing resources nor use computing resources for which you are not authorized. You may use an account only for the educational purposes appropriate for a school setting and not for other applications such as advertising for a commercial organization or running a business or activity related to running the operation of a personal business.

19. You may not reveal your password to anyone or let another person use your account unless allowed by Tioga Central's Computer Coordinator for a specific purpose.

20. You must not use the School District's network resources to gain or attempt to gain unauthorized access to remote computers.

21. You may not bypass accounting or security mechanisms or attempt to circumvent data protection schemes or uncover security loopholes including virus scan software and filter software. You must not exploit systems' weaknesses. You may not attempt to modify Tioga Central School District software, except that intended to be user-customized, without expressed permission of the School District. This requirement also

refers to desktop lay-out and status, screen savers, wall paper, printer settings, and all system settings which are specified by the Tioga Central's Computer Coordinator.

22. You may not attempt to circumvent data protection schemes or uncover security loopholes.

23. You may not deliberately perform an act, which will seriously impact the operation of computers, work stations, peripherals, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, otherwise blocking communication lines, or interfering with the operational readiness of a computer.

24. You may not change, copy, delete, read, or otherwise access system files or software without permission of the Tioga Central Computer Coordinator. In general, if it is not yours, do not touch it.

25. You may not run or install on any of the School District's computer systems, or give to another, a program, which could result in the eventual damage to a file or computer system and to the reproduction of itself. This is directed toward, but not limited to, the classes of programs known as computer viruses, Trojan horses, worms, and chain letters.

26. You may not prevent others from accessing the system nor may you unreasonably slow down the system by deliberately running wasteful jobs. Some examples include disabling or crashing the system, playing games at inappropriate sites and/or times, sending mass mailings or chain letters, creating unnecessary multiple jobs, and printing multiple or unnecessary jobs.

27. You may not deliberately perform acts, which are wasteful of computing resources or which unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, creating unnecessary multiple jobs or processes, obtaining unnecessary output, or printing or creating unnecessary network traffic. Printing **multiple copies** of any document including resumes, theses, and/or dissertations is also prohibited.

28. You must abide by the terms of all software licensing agreements and copyright laws. In particular, you must not make copies of copyrighted software, unless Tioga Central has a site license specifically allowing the copying of that software. Furthermore, you must not copy site-licensed software for the distribution to persons other than faculty, staff, and students, nor may you copy site-licensed software for use at locations not covered under the terms of the license agreement.

29. You may not use other's programs or parts thereof without proper acknowledgement. This is plagiarism and must be avoided. If you copy programs, i.e., subroutines, from a textbook or another individual, you must credit the source just as you would for a research paper. This policy applies to any material taken from a network source as well.

30. You may not distribute copyrighted or proprietary material without written consent of the copyright holder, nor violate U.S. copyright or patent laws concerning computer software, documentation, and other tangible assets. **Unless otherwise indicated by the author, you should assume that any software you did not create is copyrighted.**

31. For staff members ordering software or hardware for professional use within the confines of the School District or for your students' use within the confines of your subject area, please consult Tioga Central's Computer Coordinator for appropriate order forms, procedures, and reassurance that the software/hardware will be compatible with the technology available at Tioga Central.

32. The following types of information or software cannot be placed on any computer system at Tioga Central:

- That which infringes upon the rights of another person.
- That which is abusive, profane, or sexually offensive to the average person.
- That which consists of information, which may injure someone else and lead to a lawsuit or criminal charges. Examples of these include: pirated software, destructive software, pornographic materials, libelous statements, or communication for purposes other than educational.
- That which consists of any advertisements for personal commercial enterprises.
- E-mail accounts of any nature (hot mail, instant messaging, yahoo, etc.), which would be used for inappropriate and/or non-educational communication purposes. Refer to the **E-Mail Procedures and Acceptable Use Policy** section of this document for further e-mail guidelines.

33. You may not harass others, i.e., by sending annoying, obscene, libelous, or threatening messages. You may not provide others with programs or files that cause damage to their files or the operation of the computer system, compromise the security of their accounts, or disable their accounts.

34. You may not attempt to monitor another user's data communications, nor read, copy, change, or delete another user's files or software, without permission of the owner. For everyone's security, all staff and students must save to diskette and the diskettes, which remain the property of Tioga Central School, remain in the computer lab or under the supervision of the classroom teacher. **An alternative to saving work on disk is to save to the network drive assigned to each individual within Tioga Central's network.**

35. You may not use any of the School District's computers, workstations, or networks for work other than an educational course, research project, department activity, or for professional communications related to education. These resources may not be used for personal or financial gain. Tioga Central's computers are intended only for the specific purposes of educational use.

36. Any network traffic exiting the Tioga Central School District is subject to these acceptable use policies of the network through which it flows, as well as the policies and guidelines here. In general, commercial use of external networks is prohibited.

37. You may not use a computer system to violate any local, state, federal, or international laws including New York State statutes regarding computer crime.

38. Electronic devices, including, but not limited to, cell phones, pagers, electronic games personal data devices, IPOD's, personal CD and DVD players, are prohibited in school unless specified and supervised by the teacher in charge.

39. Tioga Central students and staff must attend an Orientation/Introduction to Computers Class at Tioga and sign and date the form acknowledging that they have read the **Policies and Procedures for Computer and Internet Use at Tioga Central**, the **Internet Protection Policy**, and the **E-Mail Procedures and Acceptable Use Policy** prior to using any of the computer facilities located within the School District. This requirement applies to all new and existing staff.

Guidelines and Policy for Internet Use at Tioga Central

Internet access is now available to students and teachers in the Tioga Central School District. In providing this service, the School District's goal is to promote educational excellence by facilitating resource sharing, innovation, and communication.

The Internet is an electronic highway connecting thousands of computers all over the world and millions of individual subscribers. Students and teacher have access to:

- Electronic mail communications with people all over the world. E-mail communication is restricted to educational/professional purposes with any student e-mail participation to be assigned and supervised by the teaching staff.
- Information and news from various organizations as well as the opportunity to correspond with those organizations.
- Public domain and shareware software of all types.
- Discussion groups on a plethora of topics ranging from Chinese culture to the environment to music to politics (as examples).
- Access to many university library catalogs, the Library of Congress, and other research organizations.

With access to computers and people all over the world also comes the availability of materials that may not be considered to be of educational value in the context of the school setting. Tioga Central School has taken available precautions to restrict access to controversial materials. However, on a global network, it is impossible to control all materials, and an industrious user may discover that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the School District.

Internet Terms and Conditions

Internet access is coordinated through a complex association of government agencies and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided so that you are aware of the responsibilities you are about to acquire. In general, this requires efficient, ethical, and legal utilization of other network resources. If a Tioga Central user violates any of these provisions, his or her account will be terminated and future access could be denied.

1. Acceptable Use – The use of your account must be in support of education and research and consistent with the educational objectives of the Tioga Central School District. Use of other organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any United States or state regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secrets. Use of the Internet for commercial activity is not acceptable. Use for product advertisement or political lobbying is also prohibited.

2. Privileges – The use of the Internet is a privilege, not a right, and inappropriate use will result in a cancellation of that privilege. You have the full responsibility for the use of your account, and under no conditions, should you share your account or your password with any other person. All recipients of accounts must participate in training pertaining to the proper use of the network. Account users are responsible for the maintenance of their accounts. A frequent review of all accounts will be conducted by Tioga Central's Computer Coordinator to determine adherence to the goals of research and education.

3. Netiquette – You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- a) Be polite. Do not get abusive in your messages to others.
- b) Use appropriate language. Do not swear, use vulgarities, or any other inappropriate language. Illegal activities are strictly forbidden.
- c) Do not reveal your personal address, phone number, and credit card number or those of any students or colleagues.
- d) Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities. Electronic mail communicates with people all over the world. E-mail communication is restricted to educational/professional purposes with any student e-mail participation to be assigned and supervised by the teaching staff.
- e) Do not use the network in such a way that you would disrupt its use by other users.
- f) All communications and information accessible via the network should be assumed to be private property. Although you delete e-mail, both sent and

received, that does not mean that it is gone. E-mailed documents may reside on servers for a long period of time.

4. The Tioga Central School District makes no warranty of any kind, whether expressed or implied, of the service it is providing. The Tioga Central School District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained is at your own risk. The Tioga Central School District specifically denies any responsibility for the accuracy or quality of information obtained through its services. Any action resulting from violation of Tioga Central's **Policies and Procedures for Computer and Internet Use and Internet Protection Policy** will be the user's responsibility and not the liability of the Tioga Central School District. It is the responsibility of each user to verify the integrity and authenticity of the information that is used.

5. **Commercial Services** – are available on the Internet. If you choose these services, you are liable for any costs that may be incurred. **Under no circumstances** may Internet access at the Tioga Central School District be used for personal financial gain by the promotion of any types of business venture or activity.

6. **Security Issues** – Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify Tioga Central's Computer Coordinator. Attempts to log into the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet.

7. **Vandalism** – Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any networks that are connected to the Tioga Central School District. This includes, but is not limited to, the uploading or creation of computer viruses as well as all hardware and furniture to which the user has access.

E-Mail Procedures and Acceptable Use Policy

Tioga Central School District

Definition and Policy

E-mail is defined as electronic mail. E-mail includes any form of electronic transmission of text, graphics, and data with or without attachments from one network user to another, local or world-wide. The communication of information through electronic services across internal and/or external networked communication resources has provided ease of use and accessibility to large volumes of data and information and a method of almost instant communication. The Tioga Central School District provides resources and services through hardware, software, network, and Internet access to its employees and students under the regulations presented in ***Tioga Central's Policies and Procedures for Computer and Internet Use***. Specifically, the following items are provided for electronic communication:

- Access to internal and external networks (i.e., the Internet)
- Access to applications, software, and specific sites residing on external networks
- Access to electronic mail accounts

As public officials of a school district, district members must exercise caution when communicating via electronic messaging services. Under the open meeting law, deliberation by a quorum of members constitutes a meeting. A quorum may be arrived at using electronic messaging without knowledge and intent by the author. School district members should use electronic mail between and among members only for communicating agenda items, meeting times, or meeting dates. Electronic mail or messaging should not be used to discuss school district matters that require public discussion under the open meeting law or risk having private information become public. Under the public records law, electronic mail and messages between public officials may be considered public record ("American School Board Association," July 2002).

E-mail is convenient and easy to use; however it may encourage casual remarks and hasty reactions. E-mails should not be considered private conversations, but rather written records and can be considered as public as meeting minutes. E-mails often end up in the public domain and can be accessed and read by others.

The use of these assets provided by Tioga Central shall be consistent with the *Policies and Procedures for Computer and Internet Use* and with the highest standards of professionalism, ethical conduct, and integrity. A violation of the standards violates the Tioga Central School District's policies. Misuse of these tools or of the use of networks, the internet, and electronic communication may result in suspension or revocation of these privileges, including employee and/or student disciplinary action.

Basics of Usage

The following items are the foundational elements of this policy and must be followed by all members of the Tioga Central School District's community (administrators, staff, students, and community members):

- Internet and e-mail access in individual classrooms must be requested in writing to the building's administrator for approval. This request must include a rationale for educational use of the Internet and/or e-mail. With the building administrator's approval, the network technician will install the necessary software to accommodate the Internet request and, in the case of e-mail, create an e-mail account and address.
- Internet access is available in Tioga Central's network computer labs. Use of this Internet and/or electronic communication falls under the same jurisdiction and policies as all use throughout the School District.
- Staff may access and use their personal e-mail accounts while at school **for educational purposes only**.
- There are no student e-mail accounts with the exception of special purpose electronic mail requests made by a teacher for his or her students (i.e., electronic penpals). These mail accounts would be created for a specific purpose, for a specific time period, and used only under the direct supervision of the teacher who assigned the project.
- If you receive e-mail and do not know who sent the e-mail or recognize its address, delete the e-mail without opening it to avoid possible virus infiltration.
- Use of network and Internet services as well as the opportunity to use electronic mail must follow the specific acceptable and unacceptable usage requirements as specified as follows in this document.

Acceptable Use of Network, Internet, and Electronic Mail Service

Acceptable use of Internet and electronic mail services provided by the Tioga Central School District includes the following:

- **Educational Use** of network services to conduct research and exchange necessary information electronically. This requirement could include electronic penpals, communication with other school districts and BOCES, or obtaining information from the State Education Department or other agency. Staff should always check with their building administrator to ascertain appropriate use of electronic communication and follow strict professional and ethical use of these services..

- **Job Related Communication** using network services in compliance with **Educational Use** to submit necessary information electronically to another educational agency. Staff should always check with their building administrator to ascertain appropriate use of electronic communication and follow strict professional and ethical use of these services.
- **Virus Software and Scanning** of all Internet files and e-mail, including attachments sent to the user. All files existing on or entering a computer, which is specifically under your supervision should have current virus protection software and scheduled scanning.

Unacceptable Use of Network, Internet, and Electronic Mail Service

Unacceptable usage of Tioga Central's network, Internet, and electronic mail services includes, but is not limited to, the following:

- Using personal electronic mail (Tioga and/or personal account) for anything **NOT** educational or job-related.
- Using Tioga Central's facilities, equipment, network, and/or hardware and software for personal financial or commercial gain.
- Using Tioga Central's facilities, equipment, and/or hardware and software for any illegal activity.
- Ignoring or preventing virus protection software and scanning of all internet files and e-mails.
- Instant messaging within Tioga Central's network or across the world-wide internet.
- Accessing remotely any off-site location Internet service for personal use or gain.
- Accessing non-educational related news groups or discussion groups.
- Intentionally degrading or disrupting equipment, software, or system performance.
- Vandalizing the data or information of another user or hardware/software provided by Tioga Central's network services.
- Gaining unauthorized access to resources or information either through unauthorized hardware connections or software manipulation.
- Invading the privacy of individuals.
- Masquerading as or using an account assigned to another user.
- Posting anonymous messages or e-mail for malicious intent.
- Posting another employee's personal/sensitive communication or e-mail without the original author's consent and/or administrator approval or without exercising good judgment and ethics.
- Downloading, storing, printing, or displaying files or messages that are profane, obscene, or the use of language or graphics, which offends or tends to degrade others.
- Downloading, storing, printing, displaying, or using music or game files.
- Placing necessary downloaded educational information in inappropriate locations on the Tioga Central School District network. [Please discuss downloading necessary information with your building administrator.]

- Transmitting school-related data and/or information over the network to non-educational sites, organizations, or individuals. No such data should ever be transmitted without the expressed written permission of the building's administrator.
- Ordering items of any kind or description unless specified as business-urgent with building administrator and business office approval.
- Loading software obtained from outside Tioga Central's standard procurement and installation channels without proper testing and approval.
- Initiating and/or forwarding electronic chain mail, greeting cards, and virus hoaxes or documents with large or non-education-related attachments.

The accessibility to external communications through Tioga Central's network and Internet services is essential, in some cases, to the nature of our educational business. However, continued access to and ease of use of Internet services and electronic communications is based on employees' adherence to professional integrity and ethical conduct with these communications. Failure to comply with the conditions set forth in this policy may result in personal suspension of the use of network services and other disciplinary action as necessary. This E-Mail Policy is in addition to and in compliance with those regulations set forth in the Tioga Central School District's *Policies and Procedures for Computer and Internet Use*.

Some Helpful Hints Regarding E-Mail Use

The following tips can help an e-mail user navigate through and avoid potential problems associated with electronic communication:

- **How you say things matters.** Choose your words carefully in every e-mail.
- **E-mail is immediate and tempts people to treat these communications casually and informally, often not professionally.**
- **E-mails are not gone even when you delete them.**
- **It does not matter what e-mail account you are using.** No matter what account you use (school or personal), what you write can be considered public record.
- **E-mails are never private .** What you write could easily fall into the hands of the public.
- **E-mails can end up in printed form and easily distributed.**
- **Don't write anything that you wouldn't want to see on the front page of the paper.**

Acknowledgements

"LMC Acceptable Use of Computing and Information Resources." Lockheed Martin Corporation. <http://protection.global.lmco.com/protection/policy/accept-use.html> .

"Policy Recommendations on E-Mail Use." The Massachusetts Association of School

Committees. 2003.

“The Perils of E-Mail.” *American School Board Journal*. American School Board Association. July 2002. www.asbj.com .

Various Public School Districts.

INTERNET PROTECTION POLICY

Internet access will be provided to students in accordance with the terms of this policy. Internet access from school computers is reserved solely for educational purposes. Use by outside groups is prohibited **with the exception of school sanctioned activities such as adult education and local community clubs where Internet use and supervision are defined and granted by the School District.** Use by student clubs and organizations is limited to those times when the Internet access points are not in use for instruction and shall be limited to educational purposes and governed by this policy. Access to the Internet will be under the direction and supervision of the staff assigned to the particular Internet access area or computer.

The School District reserves the right to monitor all Internet activity including transmission and receipt of e-mail. Use of e-mail is limited to School District and **educational purposes.**

Every computer in the School District having Internet access shall not be operated by a student unless Internet access from the computer is subject to filtering software and **supervised by the assigned staff member.** Such filtering software shall be designed and it shall operate so that images, which are obscene, pornographic, or harmful to minors, shall not be displayed. Such filtering software shall also be designed and it shall operate so that images or language, which advocates or promotes violence or hatred against particular individuals or groups of individuals or promotes the superiority of one racial, ethnic, or religious group over another shall not be displayed. For purposes of this policy, the phrase *harmful to minors* means any picture, image, graphic image file, or other visual depiction that, taken as a whole, and with respect to minors, appeals to prurient interest in nudity, sex, or excretion, depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors in actual or simulated sexual act or sexual contact, actual or simulated, normal or perverted sexual acts, or lewd exhibition of the genitals, and taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Prohibited Conduct

No student shall, while using a computer or other device connected to the Internet:

1. Access, transmit, or retransmit material which promotes violence or advocates destruction of property, including information concerning the manufacture of destructive devices, such as explosives, fireworks, smoke bombs, incendiary devices or the like.
2. Access, transmit, or retransmit any information, which is harmful to minors as that phrase is defined in this policy.
3. Access, transmit, or retransmit material which advocates or promotes violence or hatred against particular individuals or groups of individuals or advocates or promotes the superiority of one racial, ethnic, or religious group over another.
4. Use or possess bootleg software. Bootleg software means any software, which has been downloaded or is otherwise in the user's possession without the appropriate registration of the software, including the payment of any fee owing to the owner of the software.
5. Use encryption software from any access point within the School District.
6. Transmit credit card or other personal identification information, including home addresses or telephone numbers from any School District computer, without the written permission of Tioga Central's Computer Coordinator.
7. Transmit e-mail through an anonymous remailer.
8. Access the Internet from a School District computer using a non-School District Internet account.
9. Use an instant messenger service or program, Internet Relay Chat, or other forms of direct electronic communication, or enter a chat room without the express permission of the staff member supervising the computer resource.
10. Commit or attempt to commit any willful act involving the use of the network, which disrupts the operation of the network within the School District or any network connected to the Internet, including the use or attempted use or possession of computer viruses or so-called hacking or other unlawful activities on line.
11. Disable or attempt to disable filtering software. However, such filtering software may be disabled for bona fide research or other lawful purposes when the Building Principal of the building in which such research or other lawful activity will be conducted has given written permission to disable the filtering software. **The Network/Computer Technician will complete the actual disabling process.**

In addition to those penalties set forth in the student discipline code, a violation of the Internet policy may also result in loss of Internet privileges **for the duration of attendance at Tioga Central.**

Opinions, advice, services, and all other information expressed on-line are those of the on-line authors and not the School District. The Internet contains information pertaining to a variety of subjects. Not all of this information is accurate or reliable, particularly where the advice of medical, legal, accounting, or other professionals would be appropriate. Users are advised not to rely on advice found on the Internet. The School District is not responsible for such advice.

The School District does not guarantee or imply that access to the Internet will always be available when students want access or that the software provided by the District will always work as intended. The School District is not responsible for failures in the operation or technical function of the Internet or the computers or software used to access the Internet.