

## STUDENT USE OF TECHNOLOGY

The Board of Education believes that the value of information and interaction that technology offers outweighs the hazards of its misuse. Making network access available, however, carries with it the potential that some network users will encounter sources that some consider controversial or inappropriate. Because information on networks is transitory and so diverse, New Trier cannot completely predict or control what users may or may not locate. Technology provides a conduit to information; the users must be wary of the sources and content and be responsible in choosing the information to be accessed.

### **Privileges and Responsibilities**

The District's electronic network is part of the curriculum and is not a public forum for general use. Users may access technology only for educational purposes. The actions of users accessing networks through the District reflect on the School District; therefore, users must conduct themselves accordingly by exercising good judgment and complying with this policy and any accompanying administrative regulations and guidelines. Users are responsible for their behavior and communications using the District's computers and networks. Exercising this privilege requires that users accept the responsibility for all material viewed, downloaded, and/or produced.

Users will need to evaluate the validity of materials accessed through technology and cite their sources when appropriate.

The actions of users accessing networks through New Trier reflect on the School District, therefore, users must conduct themselves accordingly by exercising good judgment and complying with this policy, and any accompanying administrative regulations and guidelines.

Students who use technology will:

1. Adhere to the rules of copyright and assume that any software that they did not create is copyrighted (unless it is labeled "freeware" or "public domain").
2. Adhere to the licensing agreements governing the use of shareware.
3. Note that e-mail is not guaranteed to be private. People who operate the system do have authorization to mail; others may have access. Understand that email and network files are not private. Network administrators and other designated school officials have access to all email messages and may review files and communications to maintain system integrity and monitor responsible use.
4. Be responsible at all times for the proper use of their access privileges and for avoiding impersonations, anonymity, or unauthorized sharing of security measures or other confidential information.
5. Take responsibility for any activities using technology that is borrowed by them or under their account or password.
6. Maintain the integrity of technological resources from potentially damaging messages, physical abuse, or viruses.
7. Respect the rights of others to use equipment and therefore not use it for non-school activities.
8. Abide by the policies and procedures of networks and systems linked by technology.
9. Protect the privacy of other users and the integrity of the system by avoiding misuse of passwords, others' files, equipment and programs.

Students who use technology will not:

1. Access, submit, post, publish, display or create any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially/religiously offensive, harassing, illegal or other material unsuitable in the educational setting or unrelated to the District's educational program.
2. Interfere with, or disrupt Network use by other users; create and/or propagate unsolicited advertising, political lobbying, chain letters, pyramid schemes, computer worms, viruses, or other acts of vandalism. Vandalism includes any attempt to harm or destroy data of another user, the Internet, the District's Network or any other network. This includes, but is not limited to, uploading, downloading, creation or knowing transmission of computer viruses. If a user is uncertain whether his or her conduct is permissible, he or she should contact the System Administrator.
3. Use the account or password of another user.
4. Misrepresent themselves or others.
5. Post personal contact or other private information about oneself, a student or staff member, or otherwise invade the privacy of individuals or violating the Illinois School Student Records Act or Federal Right to Privacy Education Act.
6. Trespass in others' folders, work, or files, or gain unauthorized access to resources or entities.
7. Use the network for personal business or financial gain.
8. Forge or anonymously transmit email or other electronic materials.
9. Attempt and/or breach security measures or remove hardware/software, networks, information, or communication devices from the District or other network.
10. Damage technology, hardware and/or software.
11. Represent personal views as those of the District or those that could be interpreted as such.
12. Gain unauthorized access to resources or entities.
13. Violate copyright laws.
14. Use technology for illegal activities.
15. Use District technology while privileges have been suspended.

### **Disciplinary Actions**

Failure to comply with this policy and any administrative regulations and guidelines governing the use of technology, will result in disciplinary action by staff, administration, and/or the Board of Education.

Minimum disciplinary action will include a conference or reprimand. Additional actions as deemed appropriate will include staff/parent contact; referral to an administrator; loss of access to specific technology and/or designated area for a minimum of three school days up to 10 school days (multiple infractions or egregious misuse may result in extended or permanent loss of privileges); confiscation or inappropriate items(s); restoration/restitution; administrative and/or Board of Education action, including such serious consequences as suspension and expulsion.

### **No Expectation of Privacy**

Users must recognize that there is no assurance of confidentiality with respect to access to transmissions and files by persons outside, or from persons inside, the District. Also, New Trier reserves the right to log technology use, to monitor fileserver space utilization by users and to examine users' files and materials as needed; therefore, users cannot expect absolute privacy from District personnel as to their use of technology. (*Reference: Board Policy 7.250*)

## **Acceptable Use Regulations (AUR)**

The failure of any student to follow Board policy (above) and/or the terms of the *Acceptable Use Regulations* (below) may result in the loss of privileges, disciplinary action, and/or appropriate legal action. Students should understand that if they commit any violation, their access privileges may be revoked, and disciplinary action up to and including expulsion and appropriate legal action may be taken. **All students and parents/guardians are expected to read the terms and conditions of the Acceptable Use Regulations (below) and understand their significance.**

1. **Acceptable Use** - Access to District technology must be for the purpose of education or research, and be consistent with the educational objectives of the District.
2. **Privileges** - The use of District technology is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges and/or disciplinary action, up to expulsion. The Director of Technology in consultation with the Superintendent will make all decisions regarding whether or not a user has violated Board policy and/or its related regulations and may deny, revoke, or suspend access at any time.
3. **Unacceptable Use** – The student is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:
  - a. Knowingly using the network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or State regulation;
  - b. Unauthorized downloading of software, regardless of whether it is copyrighted or de-licensed;
  - c. Using the network for private financial or commercial gain;
  - d. Wastefully using resources, such as file space;
  - e. Hacking or gaining unauthorized access to files, resources or entities;
  - f. Intentionally invading the privacy of individuals, by the unauthorized disclosure, dissemination, or use of information about anyone that is of a personal nature;
  - g. Using another student's (or other user's) account or password;
  - h. Posting material authored or created by another without his/her consent;
  - i. Posting anonymous messages;
  - j. Using the network for commercial or private advertising;
  - k. Intentionally accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material;
  - l. Using the network while access privileges are suspended or revoked; and,
  - m. Vandalism as defined in item #11 below.
4. **Software Use**
  - a. New Trier licenses the use of copies of computer software from a variety of publishers and distributors. The District does not own the copyright to this software or its related documentation and, unless authorized by the software publisher, does not have the right to reproduce it for use on more than one computer.
  - b. According to U.S. copyright law, illegal reproduction of software is subject to civil damages of as much as \$100,000 per title infringed, and criminal penalties, including fines of as much as \$250,000 per title infringed and imprisonment of up to five years.
  - c. Students and other technology users will use the software only in accordance with the license agreement.
  - d. Students and other technology users who learn of any misuse of software or related documentation within the District will notify the Director of Technology.

5. **Network Etiquette** – Students are expected to abide by the generally accepted rules of network etiquette, including but not limited to the following:
  - a. Be polite. Do not become abusive in your messages to others.
  - b. Use appropriate language. Do not swear, or use vulgarities or any other inappropriate language.
  - c. Do not reveal the personal information, including the addresses or telephone numbers of other students.
  - d. Recognize that electronic mail (E-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.
  - e. Do not use the network in any way that would disrupt its use by other users.
  
6. **No Warranties** - The Board of Education makes no warranties of any kind, whether expressed or implied, for the service it is providing. The Board will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed-deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The Board denies any responsibility for any information, including its accuracy or quality, obtained or transmitted through use of the Internet. Further, the Board denies responsibility for any information that may be lost, damaged, altered, or unavailable when using the Internet.
  
7. **Indemnification** – The user agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this Policy including such incurred through copyright violation.
  
8. **Security** - Network security is a high priority. Keep your account and password confidential. If you can identify a security problem on the network, please notify the Director of Technology. Any user identified as a security risk may be denied access to the network.
  
9. **Use of Electronic Mail**
  - a. The District's electronic mail system, and its software, hardware, and data files, are owned and controlled by the District. The District provides e-mail to aid students in fulfilling their duties and responsibilities, and as an education tool.
  - b. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account's user. Unauthorized access by any student to an electronic mail account is strictly prohibited.
  - c. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail that would be inappropriate in a letter or memorandum.
  - d. Any message received from an unknown sender (or "SPAM") should be immediately forwarded to [spamtrap@newtrier.k12.il.us](mailto:spamtrap@newtrier.k12.il.us). Downloading any file attached to any Internet-based message is prohibited unless the user is certain of that message's authenticity and the nature of the file so transmitted.

10. **Internet Safety**
  - a. Staff members shall supervise and monitor students while students are using District Internet access.
  - b. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are (1) obscene, (2) pornographic, or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices.
  - c. The Director of Technology and staff shall monitor student and staff Internet access.
11. **Vandalism** - Vandalism will result in cancellation of privileges and other disciplinary action up and to expulsion. Vandalism is defined as any malicious attempt to harm or destroy technology or data of another user, the Internet, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.
12. **Charges** - The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs. Any and all such unauthorized charges or fees shall be the responsibility of the user.
13. **Monitoring of Personal Use** - As a condition of using the Internet, including electronic mail communication, through District computers or Internet access, users consent to monitoring and inspection by school administration of personal use of District computers. Such monitoring and inspection shall include any and all electronic mail communications made or attempted to be made or received by users and all materials downloaded by users.
14. **Copyright Web Publishing Rules** – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Web sites or file servers without explicit written permission.
  - a. For each re-publication (on a Web site or file server) of a graphic or a text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.
  - b. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Web site displaying the material may not be considered a source of permission. Permission must be in written (not electronic or verbal) form.