## TECHNOLOGY ACCEPTABLE USE REGULATIONS (AUR)

**RIGHTS AND RESPONSIBILITIES**

All use of technology will be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These Acceptable Use Regulations do not attempt to state all required or proscribed behavior by users. However, some specific examples are provided. The use of technology is a privilege, not a right.

The failure of any user to follow the terms of the Acceptable Use Regulations may result in the loss of privileges, disciplinary action up to and including suspension and/or expulsion from school, and/or appropriate legal action.

The Chief Technology Officer in consultation with the appropriate administrator will make all decisions regarding whether a user has violated Board Policy and/or these regulations and may deny, revoke, or suspend access at any time. This includes temporarily confiscating and retaining students' personal electronic devices when such devices are used to access the District's network.

**USAGE GUIDELINES**

1. **Acceptable Use** – Access to District technology and networks must be for the purpose of education or research, be consistent with the educational objectives of the District, and adhere to the regulations in this document, and in Board Policy 6-235.
2. **Unacceptable Use** – The student is responsible for his/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;
   c. Using the network for private financial or commercial gain;
   d. Wastefully using resources such as file space or bandwidth for non-educational materials;
   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. Sharing network username and/or password with another user;
   h. Using another user's account and/or password;
   i. Posting material authored or created by another without his/her consent;
   j. Posting anonymous messages;
   k. Using the network for commercial or private advertising;
   l. Intentionally accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually offensive, threatening, racially/religiously offensive, harassing, or illegal material, whether on a District-owned or student personal device;
   m. Using the network while access privileges are suspended or revoked;
   n. Vandalism as defined in item #11 below;
   o. Causing damage to technology resources, hardware, and/or software; or
   p. Removing hardware/software, networks, information, or communication devices from the District or other network.
3. **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 $150,000 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. Technology users will use the software only in accordance with the license agreement.
   d. Notify the Chief Technology Officer if you learn of any misuse of software or related documentation within the District.
4. **Network Etiquette –** Students are expected to abide by the generally accepted rules of network etiquette, whether accessing the network from a District-owned or personal device, 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 personal information, including the addresses or telephone numbers of other students.
   d. Recognize that electronic communications are not private. The District reserves the right to access all electronic communications transmitted on its networks. 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 functioning or use by others.
5. **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.
6. **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.
7. **Security** – Network security is a high priority. Keep your account and password confidential. Notify the Chief Technology Officer if you can identify a security problem on the network. Any user identified as a security risk may be denied access to the network.

8. **Use of Electronic Mail** – 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 educational tool.
    a. 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.
    b. 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. 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.
9. **Monitoring of Personal Use –** As a condition of using the Internet (including electronic messaging communication through District computers or Internet access), users consent to monitoring and inspection by school administration of personal use of District computers and personal computing and communication devices on school grounds. Such monitoring and inspection will include any and all text messages or electronic mail communications made or attempted to be made or received by users and all materials downloaded by users.
10. **Internet Safety**
    a. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are obscene, pornographic, harmful, or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or his/her designee. The Superintendent or his/her designee will enforce the use of such filtering devices.
    b. Student and staff Internet access will be monitored.
11. **Vandalism –** Vandalism will result in cancellation of privileges and other disciplinary action up to and including expulsion, and/or appropriate legal action. 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 will be the responsibility of the user.
13. **Copyright Web Publishing Rules** – Copyright law and District policy prohibit the re-publishing of text or graphics found on the Web or on the 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 verbal) form.
14. **Student Use of Mobile Devices –** Students may bring their personal communication and computing devices (i.e. cell phones, smart phones, tablets, and laptops) to school and receive the same type of filtered Internet access as on New Trier computers. In addition to the Acceptable Use Regulations, the following restrictions apply:
    a. Bypassing school security or Internet access filtering software is a violation of the usage policy.
    b. Devices may only have wireless access to the network, and may not be connected via a network cable to the school network.
    c. Devices may be used in class only with permission of the teacher.
    d. During unscheduled time, devices may be used in hallways, computer labs, study halls, and libraries unless otherwise directed by the classroom teacher or area supervisor.
    e. Devices should not be heard at any time. They must always be in silent mode, or used with headphones.
    f. Due to camera capabilities, devices are never allowed to be in sight or in use in bathrooms or locker rooms.
    g. It is a violation of the Academic Integrity Policy to have a mobile device in sight during an exam of any kind. It is expected that mobile devices be off and in backpacks during examinations, unless prior permission is given by the teacher.
    h. Inappropriate content may not reside on the device while on school grounds. That includes, but is not limited to, obscene material, material that depicts illegal or violent actions, material that may be used to threaten the safety and well-being of others, and software to facilitate breaking security systems.
    i. Students have no expectation of privacy in regard to personal devices brought onto school grounds.
    j. New Trier reserves the right to examine files and materials stored on a student's individual devices as needed to monitor acceptable use under the District's Acceptable Use Regulations.
    k. Participation in the program is at the discretion of the Chief Technology Officer and the Associate Principals; the school reserves the right to deny a student the right to bring a mobile device to school for any reason.
15. **Use of Audio and Visual Recording Devices by Students –** New Trier values the educational benefits of audio and visual recording using standalone cameras, phones, laptops, and other mobile devices. Visual recording includes picture taking and video recording. The following rules apply when using audio/visual recording devices. These guidelines do not apply to the teacher use of video conferencing technology for remote learning, but do apply to your recording the sessions.
    a. Subjects must give consent before recording or picture taking can take place.
    b. Students may record content in the classroom with the advance permission of the teacher and the written consent of the students present in the classroom. Such consent must include the signature of a parent/guardian when the student is under 18.
    c. Recordings made on school grounds or at any school sanctioned activity may not be distributed or posted on a public forum, and can only be used for individual educational purposes.
    d. If a student's IEP or 504 plan specifies that a student may use a recording device, teacher consent is not required, although the student must notify the teacher at the beginning of the term. The student will only be permitted to record the teacher's presentation of materials, and will not record any student participation.
    e. Live streaming by students in the building or when at school related events/activities is strictly prohibited.
16. **Technology Equipment Checkout –** Laptops, cameras, tripods, hard drives, and other items are available for student checkout. A student ID is required. In addition to the Acceptable Use Regulations,

the following restrictions apply:

a. Students must return equipment to the specified location by the specified time.
b. Students are responsible for any physical damage to the laptops they have checked out.
c. No food or drinks are allowed near the equipment.
d. Students may not lend equipment to other(s) or leave the equipment unattended.
e. Netbooks may be used in class only with permission of the teacher.
f. Daily fines are assessed for the late return of equipment.
g. After ten (10) days of daily fines, the equipment is considered lost and a fine to cover the cost of equipment replacement is assessed.
h. Checkout renewal is at the discretion of District staff.

**STUDENT ONLINE PUPIL PRIVACY ACT (SOPPA)**

School districts throughout the State of Illinois contract with different educational technology vendors for beneficial K-12 purposes such as providing personalized learning and innovative educational technologies, and increasing efficiency in school operations.

Under Illinois' Student Online Personal Protection Act, or SOPPA (105 ILCS 85/), educational technology vendors and other entities that operate Internet websites, online services, online applications, or mobile applications that are designed, marketed, and primarily used for K-12 school purposes are referred to in SOPPA as operators. SOPPA is intended to ensure that student data collected by operators is protected, and it requires those vendors, as well as school districts and the Ill. State Board of Education, to take a number of actions to protect online student data.

Depending upon the particular educational technology being used, our District may need to collect different types of student data, which is then shared with educational technology vendors through their online sites, services, and/or applications. Under SOPPA, educational technology vendors are prohibited from selling or renting a student's information or from engaging in targeted advertising using a student's information. Such vendors may only disclose student data for K-12 school purposes and other limited purposes permitted under the law.

In general terms, the types of student data that may be collected and shared include personally identifiable information (PII) about students or information that can be linked to PII about students, such as:

- Basic identifying information, including student or parent/guardian name and student or parent/guardian contact information, username/password, student ID number
- Demographic information
- Enrollment information
- Assessment data, grades, and transcripts
- Attendance and class schedule
- Academic/extracurricular activities
- Special indicators (e.g., disability information, English language learner, free/reduced meals or homeless/foster care status)
- Conduct/behavioral data
- Health information
- Food purchases
- Transportation information
- In-application performance data
- Student-generated work
- Online communications
- Application metadata and application use statistics
- Permanent and temporary school student record information

Operators may collect and use student data only for K-12 purposes, which are purposes that aid in the administration of school activities, such as:

- Instruction in the classroom or at home (including remote learning)
- Administrative activities
- Collaboration between students, school personnel, and/or parents/guardians
- Other activities that are for the use and benefit of the school district