
TECHNOLOGY ACCEPTABLE USE POLICY

Integrating technology into the curriculum is a priority. Technology should be integrated, not as a separate subject or as a once-in-a-while project, but as a tool to promote and extend student learning on a daily basis. The challenge is in finding ways to use technology -- and to help students use it -- that don't take time away from core subjects. We need to prepare our students

MISSION STATEMENT

It is the mission of the Thousand Islands School District to integrate technology into curriculum, instruction, and assessment in order to:

1. Provide opportunities for active, collaborative, individualized, and interdisciplinary learning.
2. Provide a multimedia learning environment that includes global communication and information exchange.
3. Prepare students to function in a technological world.
4. Prepare students to make a smooth transition to the worlds of college and work.
5. Enhance teacher and student communication skills.
6. Provide the entire learning community with opportunities to become technologically literate.

VISION STATEMENT

Technology at the Thousand Islands School District is a vehicle by which the school community learns, communicates and creates.

Our vision is that technology will allow us to expand our reach within the community.

Technology will enable us to leverage increased collaboration among staff and through better access to information and each other we will be able to improve our delivery of services.

Students will take greater advantage of the social and academic opportunities we provide. The proper use of technology within the district will allow us to become more efficient and effective in our day-to-day tasks leading to better service for the school community.

GUIDELINES

It is imperative that staff, students, and visitors conduct themselves in a responsible, and legal manner while using District equipment and networks. This policy provides general guidelines for use by its users. Final determination of acceptable behavior rests with the Superintendent. The following factors define District policy for Computer Network and Internet access:

- A. Any use of District equipment or computer networks for inappropriate, illegal, obscene, or sexually exploitive purposes is prohibited. Illegal activities are defined as any violation of local, State and Federal laws as well as any violation of the District's established rules and regulations governing appropriate behavior. Inappropriate use is defined as any violation of the intended purpose to which the network access account was issued. Obscene activities are defined as any violation of generally accepted social standards for use of publicly operated communication medium, which is accessible, by children and underage adults;
- B. Any use of the District's equipment for commercial purposes, or individual profit is prohibited;
- C. Any use of the District's equipment for partisan political activity is prohibited;
- D. Any use of the District's equipment that is intended to disrupt use by other users, deny intended services, or invade the privacy of others is prohibited;

- E. The District's network accounts shall be used only by authorized students and staff as approved by the building principal/district administrators. Users are solely responsible for all activity that occurs while logged in under their operating or individual accounts;
- F. It is expected that all users will prudently use the District's resources and prevent waste wherever possible. Users may not intentionally write, produce, generate, copy, propagate, or attempt to introduce any computer code designed to self replicate (e.g., computer virus), damage or otherwise hinder the performance of any computer's memory, file system, or software;
- G. Users may not intentionally tamper with networks, terminals, printers, wiring, etc., or attach unauthorized devices or equipment to the network. Installation, modification, or removal of software will be done only under the supervision of a qualified technician and with the approval of the network administrator and the district technology coordinator;
- H. Students, staff, parents, and administrators are prohibited from disclosing student records, personnel information, confidential records, or internal financial data to unauthorized recipients;
- I. Any user's network communications that traverses another network is subject to that network's acceptable use policy;
- J. Student use is permitted with appropriate administrative authorization, and proper supervision;
- K. Users must recognize and observe applicable copyright laws and usage restrictions. Unauthorized duplication, deletion, alteration, or reconfiguration of District software, or any other activity deemed an infringement of a product copyright is prohibited;
- L. All data and other work created, stored, or maintained on District computing resources is the property of the District. Users are not permitted to inappropriately delete stored information, regardless of authorship, or to otherwise alter access to their computing resources in a manner which would deny the District access to historical information or which would otherwise impede normal functioning of the business of the District;
- M. The District reserves the right to read and/or access users' files when necessary to resolve problems reported by the owner of those files, or in similar situations with the knowledge and consent of the owner. Access to a user's directory and files may be necessary to remove extraneous files from the system or verify proper system operation, or to effectuate fixes and upgrades, or to comply with bona fide investigations. When access is required without the knowledge and consent of the owner, the activity will be logged by the building Technology representative, along with the reasons for access, for review by the Superintendent;
- N. Access to District computing resources shall terminate upon student graduation and employee termination of employment. Accounts may stay active at the discretion of the Superintendent.
- O. Each building Principal (or his/her designated representative) is the first level of responsibility to review alleged infractions of this policy and will coordinate with District staff to determine appropriate corrective action. The Principal shall notify the District Technology Coordinator when and if an account needs to be disabled due to the infraction;
- P. The Superintendent is the final authority on the resolution of any conflicts between this policy and other established procedures. The Superintendent is the final decision authority on all matters related to the District Computer Network.

Guidelines for Publishing Student work, Images and Names

No personal information about students or their parents/guardians, including phone numbers, home addresses or e-mail addresses shall be published on a District or school web page.

Student Images:

- Students are routinely videotaped & photographed during school concerts, assemblies, awards, classroom activities, etc.
- These images may be displayed or shown on the Thousand Islands Central School District's web site.
- Student names are not connected with their images.

Student Names / Work:

Recognizing a student's accomplishments through appropriate publicity shares the good news of a student's achievement and can build or reinforce his/her positive self-image.

- When original student work is posted without an accompanying student picture, a student's first name and, if necessary for clarification, grade designation may be cited (e.g. Kathy, grade 7a, John, grade 4) without specific notification.

Parents who do not want their child videotaped or photographed and those images displayed in the circumstances described are asked to contact the school.

SANCTIONS

- A. Violations may result in loss of access. Users involved will be informed of the nature of these violations, and will have an opportunity to respond to them;
- B. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior;
- C. Users may be required to make full financial restitution;
- D. When applicable, law enforcement agencies may be involved.

START-UP SCREEN NOTICE

The following statement shall be displayed upon startup, "Your use of the workstation implies that you have read, understand and agree to abide by the Thousand Islands School District's Acceptable Use Policy for access to the device."

INTERNET SAFETY POLICY – see appendix A

- I. A. Although the Thousand Islands Central School District recognizes the value of the Internet as an educational tool, it also understands that information with no redeeming social value is accessible through the internet.
- B.
 1. The Thousand Islands Central School District has developed and will enforce this Internet Safety Policy in compliance with the Children's Internet Protection Act (CIPA) and the Neighborhood Children's Internet Protection Act (NCIPA).
 2. In addition, the Thousand Islands Central School District maintains its "Computer and Internet Use Policy", which governs the acceptable use of the Internet by students and employees.

II. Access to the Internet using the Thousand Islands Central School District's computer equipment is subject to the following restrictions:

A. **Filtering.** Filtering software will be used to block minors' access to: (Appendix A)

1. Visual depictions that are (a) obscene, (b) child pornography, or (c) harmful to minors; and
2. Internet sites which, in the Board's determination, contain material which is "inappropriate for minors."

Adult access to visual depictions that are obscene and/or child pornography will also be blocked. However, the Superintendent or his/her designee may disable the software to enable access to blocked sites for bona fide research or other lawful purposes.

B. **Safety of Minors When Using Direct Electronic Communications.**

1. In using the computer network and Internet, minors are not permitted to reveal personal information such as home addresses, telephone numbers, their real last names or any information which might allow someone they are communicating with online to locate them. No minor may arrange a face-to-face meeting with someone he/she "meets" on the computer network or Internet without his/her parent's permission.
2. Before utilizing any electronic communications (including but not limited to electronic mail and "chat rooms") in any instructional setting, students will be taught that they must disclose to their teacher any message they receive that is inappropriate or makes them feel uncomfortable. They must also be taught that they must never agree to meet with someone they have met online without their parents' approval.

C. **Unauthorized Access and Other Unlawful Activities.** It is a violation of this Policy to:

- a. use the Thousand Islands Central School District's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access;
- b. damage, disable or otherwise interfere with the operation of computers, computer systems, software or related equipment through physical action or by electronic means; and/or
- c. violate state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or any other applicable law or municipal ordinance.

D. **Unauthorized Disclosure and Dissemination of Personal Identification Information Regarding Minors.** Personally identifiable information concerning minors may not be disclosed on the Internet (e.g. On the Thousand Islands Central School District 's web page" without the permission of a parent or guardian. If a student is 18 or over, the permission may also come from the student himself/herself.

III. **Regulations and Dissemination.** The Superintendent is authorized to develop and implement regulations consistent with the policy. The Superintendent will also be responsible for disseminating the policy and associated regulations to school personnel and students.

HOME AND SCHOOL ACCESS

The Family Education Rights and Privacy Act, FERPA, also known as the Buckley Amendment of 1974, requires the confidentiality of students' records, and the personally identifiable information contained in them. Absent of written permission from the parent or information published as Directory Information, the accessing of student records can only be for legitimate educational interests, or the need-to-know exception, in fulfilling one's professional responsibilities. With staff's capability of easily accessing student records via the SchoolTool student information system, great care and caution must be exercised in the utilization and dissemination of information. It is imperative that one's access and pass code to SchoolTool data be protected at all times. The accessing of students' demographics i.e. address or free and reduced meal eligibility for the purposes of mailings, recruitments, or scholarships is limited and it can be authorized via one's administrator.

Appendix A

Generally speaking, "**obscenity**" is defined as any work that an average person (applying contemporary community standards) would find, taken as a whole, appeals to a prurient interest. The work also must depict or describe, in a patently offensive way, sexual conduct as specifically defined in state law. Moreover, the work, taken as a whole, has to lack serious literary, artistic, political or scientific value.

"**Child Pornography**" is defined as:

...any visual depiction, including a photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of visual depiction involves the use of a minor (someone under the age of 19) engaging in sexually explicit conduct; (b) such visual depiction is or appears to be, of a minor engaging in sexually explicit conduct; (c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (d) such visual depiction is advertised, promoted, presented, described or distributed in such manner conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

The phrase "**harmful to minors**" is defined as:

...any picture, graphic image, file, or other visual depiction that (a) taken as whole and with respect to minors (defined here as anyone under the age of 17), appears to a prurient interest in nudity, sex or excretion; (b) depicts, describes, or presents, 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 genitals; and (c) taken as a whole, lacks serious literacy, artistic, political, or scientific value as a to minors.

VIOLATIONS/CONSEQUENCES:

Students:

- (a) Students who violate this policy shall be subject to loss of district system access up to and including permanent loss of privileges, and discipline up to and including expulsion.
- (b) Violations of law will be reported to law enforcement officials.
- (c) Disciplinary action may be appealed by parents and/or students in accordance with existing district procedures for suspension or loss of student privileges.