Thousand Islands CSD

Technology Acceptable Use Policy

Grades K-12

2018-2019

www.1000islandsschools.org

Acceptable Use Policy
Thousand Islands Central School District (TICSD) makes a variety of communications and information technologies available to students and staff through computer/network/Internet access. These technologies, when properly used, promote educational excellence in the District by facilitating resource sharing, innovation, and communication. Illegal, unethical or inappropriate use of these technologies can have dramatic consequences, harming the District, its students and its employees. This Acceptable Use policy is intended to minimize the likelihood of such harm by educating District users and setting standards which will serve to protect the District. The District firmly believes that digital resources, information and interaction available on the computer/network/Internet far outweigh any disadvantages.

Mandatory Review
To learn proper computer/network/Internet use and conduct, students and staff are required to review these guidelines at the beginning of each school year. All District users shall be required to acknowledge receipt and understanding of all guidelines governing use of the system and shall agree to allow monitoring of their use and to comply with such guidelines. The parent or legal guardian of a student user is required to acknowledge receipt and understanding of the District's Acceptable Use policy as part of their review of the Parent and Student handbook.

This policy will be reviewed and updated as needed annually by the TPC committee and approved by the Board of Education in order to keep this policy current.

Digital Citizenship *
Digital citizenship can be defined as the norms of appropriate, responsible behavior with regard to technology use. All users are expected to be aware of and adhere to these elements.
Digital Access: full electronic participation in society.
Technology users need to be aware that not everyone has the same opportunities when it comes to technology. Working toward equal digital rights and supporting electronic access is the starting point of Digital Citizenship. Digital exclusion makes it difficult to grow as a society which increasingly use these tools. Helping to provide and expand access to technology should be goal of all digital citizens. Users need to keep in mind that there are some that may have limited access, so other resources may need to be provided. To become productive citizens, we need to be committed to make sure that no one is denied digital access.

Digital Commerce: electronic buying and selling of goods.
Technology users need to understand that a large share of market economy is being done electronically. Legitimate and legal exchanges are occurring, but the buyer or seller needs to be aware of the issues associated with it. The mainstream availability of Internet purchases of toys, clothing, cars, food, etc. has become commonplace to many users. At the same time, an equal amount of goods and services, which are in conflict with the laws or morals of some countries, are surfacing. (This might include activities such as illegal downloading, pornography, and gambling. Users need to learn about how to be effective consumers in a new digital economy.

Digital Communication: electronic exchange of information.
One of the significant changes within the digital revolution is a person's ability to communicate with other people. In the 19th century, forms of communication were limited. In the 21st century, communication options have exploded to offer a wide variety of choices (e.g., e-mail, cellular phones, instant messaging). The expanding digital communication options have changed everything because people are able to keep in constant communication with anyone else. Now everyone has the opportunity to communicate and collaborate with anyone from anywhere and anytime. Unfortunately, many users have not been taught how to make appropriate decisions when faced with so many different digital communication options.

Digital Literacy:
Process of teaching and learning about technology and the use of technology.
While schools have made great progress in the area of technology infusion, much remains to be done. A

renewed focus must be made on what technologies must be taught as well as how it should be used. New technologies are finding their way into the work place that is not being used in schools (e.g., Videoconferencing, online sharing spaces such as wikis). In addition, workers in many different occupations need immediate information (just-in-time information). This process requires sophisticated searching and processing skills (i.e., information literacy). Learners must be taught how to learn in a digital society. In other words, learners must be taught to learn anything, anytime, anywhere. Business, military, and medicine are excellent examples of how technology is being used differently in the 21st century. As new technologies emerge, learners need to learn how to use that technology quickly and appropriately.
Digital Citizenship involves educating people in a new way— these individuals need a high degree of information literacy skills.

Digital Etiquette:
Electronic standards of conduct or procedure.
Technology users often see this area as one of the most pressing problems when dealing with Digital Citizenship. We recognize inappropriate behavior when we see it, but before people use technology they do not learn digital etiquette (i.e., appropriate conduct). Many people feel uncomfortable talking to others about their digital etiquette. Often rules and regulations are created or the technology is simply banned to stop inappropriate use. It is not enough to create rules and policy, we must teach everyone to become responsible digital citizens in this new society.

Digital Law:
Electronic responsibility for actions and deeds
Digital law deals with the ethics of technology within a society. Unethical use manifests itself in form of theft and/or crime. Ethical use manifests itself in the form of abiding by the laws of society. Users need to understand that stealing or causing damage to other people's work, identity, or property online is a crime. There are certain rules of society that users need to be aware in an ethical society. These laws apply to anyone who works or plays online. Hacking into others information, downloading illegal music, plagiarizing, creating destructive worms, viruses or creating Trojan Horses, sending spam, or stealing anyone's identify or property is unethical.

Digital Rights and Responsibilities:
Those freedoms extended to everyone in a digital world.
Just as in the American Constitution where there is a Bill of Rights, there is a basic set of rights extended to every digital citizen. Digital citizens have the right to privacy, free speech, etc. Basic digital rights must be addressed, discussed, and understood in the digital world. With these rights also come responsibilities as well. Users must help define how the technology is to be used in an appropriate manner. In a digital society these two areas must work together for everyone to be productive.

Digital Health and Wellness:
Physical and psychological well-being in a digital technology world. Eye safety, repetitive stress syndrome, and sound ergonomic practices are issues that need to be addressed in a new technological world. Beyond the physical issues are those of the psychological issues that are becoming more prevalent such as Internet addiction. Users need to be taught that there inherent dangers of technology. Digital Citizenship includes a culture where technology users are taught how to protect themselves through education and training.

Digital Security:
Electronic precautions to guarantee safety. In any society, there are individuals who steal, deface, or disrupt other people. The same is true for the digital community. It is not enough to trust other members in the community for our own safety. In our own homes, we put locks on our doors and fire alarms in our houses to provide some level of protection. The same must be true for the digital security. We need to have virus protection, backups of data, and surge control of our equipment. As responsible citizens, we must protect our information from outside forces that might cause disruption or harm.

*Ribble, Mike "Nine Themes of Digital Citizenship." Digital Citizenship: Using Technology Appropriately. GoDaddy, 2013. <http://digitalcitizenship.net/Home_Page.html>.

Guidelines:
This Acceptable Use Policy outlines the guidelines and behaviors that users are expected to follow when using TICSD technologies.
•The network is intended for educational purposes.
•All activity over the network or using district technologies may be monitored and retained.
•Access to online content via the network may be restricted in accordance with TICSD policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
•Students and staff are expected to follow the same rules for good behavior and respectful conduct online as offline.
•Misuse of school resources can result in disciplinary action.
•TICSD makes a reasonable effort to ensure students' safety and security online, but will not be held accountable for any harm or damages that result from misuse of school technologies.
•Users of the network or other technologies are expected to alert the tech staff immediately of any concerns for safety or security.

Technologies Covered
TICSD may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.
•As new technologies emerge, TICSD will attempt to provide access to them along with appropriate education as needed. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies
All technologies provided by TICSD are intended for educational purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; don't try to get around technological protection measures; use good common sense; and ask if you don't know.

Web Access
TICSD provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Web browsing may be monitored and web activity records may be retained indefinitely.
•Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert a tech staff member or submit the site for review.

Email

TICSD may provide users with email accounts for the purpose of school-related communication. Availability and use may be restricted based on school policies.
•If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed by the district policy or the teacher.
•Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage is monitored and archived. There should be no expectations of privacy. District management and or his/her designee has the right to review email at their discretion.
•A Disclaimer will be attached to all TICSD owned E-Mail:

- Pursuant to School Board policy and administrative procedures, this e-mail system is the property of the Thousand Islands Central School District and is to be used for official business only. In addition, all users are cautioned that messages sent through this system may be subject to the Freedom of Information Law and other laws of the State of New York and also to review by the school system. There should be no expectation of privacy when sending or receiving e-mails.

Social / Web 2.0 / Collaborative Content
•Recognizing that collaboration is essential to education, TICSD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.
•Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices Policy
TICSD may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.
•Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to tech staff immediately. Users may be financially accountable for any damage resulting from negligence or misuse.
•Use of school-issued mobile devices, including use of the school network, may be monitored.

Personal Electronic Devices (PED)
The display and/or use by student's grades K-12 of personal electronic devices shall be prohibited from the time students arrive at school until the end of the regular school day. Grades Six to Twelve students' electronic devices are to be off and in lockers from 7:35 a.m. to 2:30 p.m.
•Examples of a personally owned device shall include but is not limited to: MP3 players and iPods; iPads, Nooks, Kindle, headphones, and other tablet PCs; laptop and netbook computers; personal digital assistants (PDAs), cell phones and smart phones such as iPhone and/or Droids, as well as any gaming devices, and other devices with similar capabilities.
•If any school staff member hears a cell phone, ipad, ipod, or any other electronic device ring in a backpack or locker, they have the right to search the backpack or locker and take the device to the office.

Violations to Personal Electronic Devices (PED) Policy
•1st electronic device violation will result in the device being taken to the office and may be picked up by the student at the end of the day

•2nd electronic device violation, the device will be brought to the office, the student will serve a one-hour after school or a one-hour in school detention, and a parent/guardian will be notified that they need to pick up the device in the office.
•3rd offense, the student will not be allowed to bring any electronic devices to school, the device will be brought to the office, the student will serve a one day In-School Suspension (ISS), and a parent/guardian will need to pick the phone up in the office.
•4th offense, the student will not be allowed to bring any electronic devices to school, the device will be brought to the office, a parent/guardian will need to pick the phone up in the office, and a Superintendent's Hearing will be scheduled.

Security
Users are expected to take reasonable safeguards against the transmission of security threats over the school network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert the tech staff. Do not attempt to remove the virus yourself or download any programs to help remove the virus.
•Create strong passwords and change passwords regularly.

Guidelines for Publishing Student Work, Images, and Names
The district has an obligation to protect student safety and to balance this with the need for open communications when using the Internet.

•No personal information about students or their parents/guardians (beyond first names or nicknames), including phone numbers, home addresses or e-mail addresses shall be published on the District web page.
•Students are routinely video recorded and photographed during school concerts, assemblies, awards, classroom activities, etc. These images may be displayed or shown on the TICSD web site. When student images are posted, only first names or nicknames will be referenced.
•Comments on student work will be moderated by the teacher to ensure only appropriate information is shared and received.
•Online safety and appropriate behavior will be emphasized whenever sharing student work online.
•It is clear that there are significant risks, as well as significant advantages, involved with allowing students to be identified on the Internet. Therefore, students should not be easily identifiable from materials they or the school system might publish on the Internet. No directory information will be posted on the Web for students whose parents have indicated, in writing, that such information not be released.

Staff that publish and manage a classroom web page for instructional use are solely responsible for the content of that particular site. The use of District web pages for the purpose of publishing is a privilege, not a right, and misuse will result in the restriction or cancellation of the account. No student will be given or have access to publish on District webpages.

Downloads
Users will not download or attempt to download or run .exe programs over the school network or onto school resources without express permission from the Technology Director. You may be able to download other file types, such as images or videos. For the security of the TICSD network, download such files only from reputable sites, and only for educational purposes.

Netiquette
Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

•Users should also recognize that among the valuable content online that there is also unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.
•Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways you never intended.

Plagiarism
Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet.
•Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety
If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.
•Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission.
•Users should recognize that communicating over the Internet decreases anonymity and increases associated risks. Users should carefully safeguard the personal information of themselves and others.
•Users should never agree to meet someone they meet online in real life without parental permission.
•Users should create strong passwords and change passwords regularly.
•Users will not share their password(s) with anyone.
•Users will not use another users account(s) or password(s).

Cyberbullying
Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.
•Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges as outlined in the student code of conduct. In more frequent cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.
•All students are expected to promptly report violations to a teacher, guidance counselor, the building principal, or other school personnel. All district staff is expected to promptly report violations to their supervisor who shall in turn impose an appropriate disciplinary sanction, if so authorized; or refer the matter to a staff member who is authorized to impose an appropriate sanction. The building principal or his or her designee must notify, within 24 hours, the appropriate local law enforcement agency and parents of those code violations that constitute a crime and substantially affect the order or security of a school. The notification to parent may be made by telephone, followed by a letter mailed on same day as the telephone call is made. The notification must identify the student and explain the conduct that violated the code of conduct and constituted a crime.

Bullying/harassment that occurs off campus are expected to be reported where such acts:
•Create or would foreseeably create a risk of substantial disruption within the school environment
•Where it is foreseeable that the conduct, threats, intimidation or abuse might reach school property
•This reinforces the importance of reporting incidents of discrimination and harassment. Incidents of discrimination or harassment including bullying shall be reported using the Thousand Islands School District's Dignity for All Students (Discrimination, Harassment, and Bullying) Reporting Form

Children Under 13
In order to comply with the Children's Online Privacy Protection Act, the TICSD will not knowingly allow a child under the age of 13 to create an account without parental consent.

Student Data Breach
School Districts have a legal responsibility to protect the privacy of education data, including personally identifiable information (PII) of its students, in both paper and electronic formats. Although the Family Education Rights and Privacy Act (FERPA) does not include specific data breach notification requirements, it does protect the confidentiality of education records by requiring districts to record each incident of unintentional data disclosure. Authorized access of personal information by a Thousand Islands Central School District employee, with a legitimate educational interest in the data or information, is not considered a breach of the security of the system, provided the personal information is not used or subject to further unauthorized disclosure. A breach of student data maintained electronically would be considered such a "disclosure" that must be recorded. In addition, under state law, direct notification to parents and/or affected students may be warranted depending on the type of data compromised, such as student social security numbers and/or other identifying information that could lead to identity theft.
The following guidelines will assist the School District in efforts to prevent student data breaches and guide the response and notification protocol should a student data breach occur.

Definitions
•"Data Breach" is any instance in which there is an unauthorized release of or access to Personally Identifiable Information (PII) from student education records or other protected information about students not suitable for public release.
•"Education Records" are records directly related to a student and maintained by an education agency or institution, or by a party acting on behalf of the agency or institution.

•"Personally Identifiable Information (PII)" from education records includes information, such as a student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. PII includes an individual's name, identification number, social security number, date and place of birth, mothers' maiden name, biometric records, etc.

Prevention of Student Data Breaches Incident Response Team
The District may choose to assemble an incident response team within the District to deal with possible data breaches. The team may designate a manager who will be in charge of incident response and at least one (1) other person who can assume authority in the absence of the manager. Staff will be notified of the team and the method of contact in the event of a breach. The team will also be available to staff to answer questions and develop strategies to prevent and detect a breach. The team will establish roles and responsibilities, specify access credentials, work with the Superintendent to coordinate the flow of information, and manage the District's public message in the event of a breach.

Review Information Systems and Data
- The District, in conjunction with appropriate staff will review information systems and data to identify where personally identifiable information (PII) is stored and used. The review may involve:
- Documenting what PII and other sensitive information is maintained by the District, where it is stored (including backup and archived data), and how it is kept secure;
- Conducting regular risk assessments and evaluating privacy threats for the District;

- Reviewing those approved for access to PII and/or other sensitive information and checking user activity status to determine which accounts should be deactivated after a pre-determined period of inactivity;
- Reviewing separation of duties to help ensure integrity of security checks and balances;
- Implementing mitigation controls designed to prevent and detect unauthorized access, theft, or misuse of PII and/or other sensitive data;
- Implementing security controls, such as encryption of sensitive data in motion and at rest (where feasible); and
- Regularly reviewing and updating data destruction policies to minimize the risk of data breaches through unauthorized access to archived records or computers that are no longer in use.

Monitor Sensitive Data Leakage and Loss

The District will also monitor for PII and other sensitive data leakage and loss. This may include:
1)Employing automated tools, such as intrusion detection and prevention systems, next generation firewalls, and anti-virus and anti-malware tools, to monitor and alert about suspicious or anomalous activity;
2)Using data loss prevention solutions to track the movement and use of information within the District's system, to detect and prevent the unintentional disclosure of PII and/or other sensitive data, for both data at rest and data in motion;
3)Conducting regular searches of the information system and physical storage areas to identify PII that may be outside of approved areas (i.e., scan networks for policy violations or occasionally police open areas for PII left unattended on desks);
4)Periodically testing and checking privacy and information security controls (i.e., through the use of "real-life" exercises) to validate their effectiveness as part of a risk management program.

Conduct Privacy and Security Awareness Training

The District may conduct privacy and security awareness training. This may include:
1)Providing privacy and information security training on a recurring basis to appropriate staff involved in data-related activities;

2)Posting and communicating privacy policies to parents, students, staff and other users (i.e., on the District Web page, on a bulletin board at the office, or through statements inserted in documents or emails, etc.); and
3)Clearly defining and making easily accessible processes for reporting privacy incidents and complaints.

Response to Student Data Breaches

In the event that information from student education records may have been compromised or inadvertently disclosed, the District may take one or more of the following steps suggested by the U.S. Department of Education, as deemed necessary under the particular circumstances. The following list is not meant to be linear or all inclusive:
1)Validate or confirm the data breach and determine exactly what information was compromised (i.e., names, addresses, social security numbers, ID numbers, credit card numbers, grades, and the like).
2)Assemble an incident response team to coordinate all aspects of the breach response.
3)Take steps immediately to determine affected devices, retrieve data, and prevent any further disclosures.
4)Identify all affected records and students. Locate, obtain, and preserve for examination all written and electronic logs and records applicable to the breach.
5)Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised. Determine whether the incident occurred because of a lack of monitoring and oversight.

6)Determine whether institutional policies and procedures were breached, including organizational requirements governing access (user names, passwords, PINs, etc.); storage; transmission; and destruction of information from education records.
7)Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.
8)Consult with the District's School Attorney to ensure compliance with any applicable federal, state and/or local laws or regulations related to data breaches, reporting or notification requirements.
9)Report the incident to law enforcement authorities if criminal activity is suspected. If law enforcement is involved, coordinate investigations and evidence collection to avoid compromising outcomes.

Notification of Student Data Breaches
•In the event of a student data breach, the District will determine whether notification is warranted or required and when it should be made, pursuant to federal, state, and local laws. If the compromised data includes student social security numbers in combination with other identifying information that could lead to identity theft, the District may directly notify affected students and/or their parents of the breach and notify students and their parents that the U.S. Education Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at:
http://www.ed.gov/about/offices/list/oig/misused/idtheft.html and
http://www.ed.gov/about/offices/list/oig/misused/victim.html.
•The District shall maintain a record of each incident of data disclosure in accordance with 34 CFR 99.32 (a)(1).
•Consider Notification of FPCO and PTAC
•The incident response team may consider notifying the Family Policy Compliance Office (FPCO) about the breach. The FPCO can assist School Districts by helping to determine the potential for harm from the release of the information. The incident response team may also consider seeking technical assistance from the Privacy Technical Assistance Center (PTAC) for support with security and breach prevention
•If the breach involves student data protected under state law, or data other than student educational records, refer to Policy #5440 INFORMATION SECURITY BREACH AND NOTIFICATION.

Examples of Acceptable Use
I will:
•Use school technologies for school-related activities and research.
•Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
•Treat school resources carefully, and alert staff if there is any problem with their operation.
•Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
•Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
•Use school technologies at appropriate times, in approved places, for educational pursuits only.
•Cite sources when using online sites and resources for research; ensure there is no copyright infringement.
•Recognize that use of school technologies is a privilege and treat it as such.
•Be cautious to protect the safety of myself and others.
•Help to protect the security of school resources.
This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Unacceptable Use
I will not:
•Use school technologies in a way that could be personally or physically harmful to me or others.
•Search inappropriate images or content.

•Engage in cyberbullying, harassment, or disrespectful conduct toward others–staff or students.
•Try to find ways to circumvent the school's safety measures and filtering tools.
•Use school technologies to send spam or chain mail.
•Plagiarize content I find online.
•Use copyrighted material I find online.
•Post personally-identifying information, about myself or others.
•Agree to meet someone I meet online in real life.
•Share passwords with anyone.
•Use another users account or password.
•Use language online that would be unacceptable in the classroom.
•Use school technologies for illegal activities or to pursue information on such activities.
•Attempt to hack or access sites, servers, accounts, or content that isn't intended for my use.
This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability
TICSD will not be responsible for damage or harm to persons, files, data, or hardware. While TICSD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. TICSD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Violations of the Acceptable Use Policy
Violations of this policy may have disciplinary repercussions as outlined in the student code of conduct.
The School District reserves the right to:
1.Determine which CIS systems' services will be provided through School District resources.
2.Determine the types of files that may be stored on School District file servers and Computers.
3.View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and Electronic Communications Systems, including e-mail and other Electronic Communications.
4.Remove excess e-mail and other Electronic Communications or files taking up an inordinate amount of fileserver space after a reasonable time.
5.Revoke User privileges, remove User accounts, or refer to legal authorities and/or School District authorities when violation of this and any other applicable School District policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, data breaches, and destruction of School District resources and equipment.

Thousand Islands School District Chromebook Program

Grades 5 - 12

2018-2019

Mission:
The mission of the 1-to-1 program in the Thousand Islands School District is to create a collaborative learning environment for all learners. This environment will enable and support students and teachers to implement transformative uses of technology while enhancing students' engagement with content and promoting the development of self- directed, responsible lifelong learners and users. Students will transition from consumers of information to creative producers and owners of knowledge. The District will integrate professional development for teachers and students to enhance classroom environments by implementing high-quality instruction, assessment and learning through the use of technology and curriculum. Technology immersion does not diminish the vital role of the teacher. To the contrary, it transforms the teacher from a director of learning to a facilitator of learning.

Device Purpose:
The Thousand Islands School District is supplying students with a Chromebook device. This device is property of the Thousand Islands School District. The supplied device will provide each student access to educational materials needed for each student to be successful. The Chromebook allows student access to Google Apps for Education, educational web-based tools, as well as many other useful sites. The supplied device is an educational tool not intended for **gaming, social networking, or entertainment**.

Receiving your Chromebook:
District Owned/Issued Chromebooks will be distributed within the first week after the start of school each year to High School students. Middle School students will have Chromebooks slated for them in their classrooms. Parents/Guardians and students MUST sign and return the Chromebook Agreement document before the Chromebook can be issued to their child. This Chromebook Policy outlines the procedures and policies for student use and for students and families to protect the Chromebook investment for the Thousand Islands School District. Chromebooks will be collected at the end of each school year and students will be reissued the same Chromebook every year while they are still enrolled in the same building.

Returning your Chromebook:
All district owned Chromebooks must be returned following the guidelines in their respective school buildings.
●Students leaving the District must return district owned Chromebooks to the office of their school.
●Chromebooks will be collected during the last week of school for summer maintenance.
●Any Chromebook not returned at the end of the year or when the student is no longer enrolled will be considered stolen property and law enforcement agencies will be notified if payment for missing device is not received.
●Chromebooks will be examined for damage and fees will be issued if damage is found to be beyond normal wear and tear.

General Guidelines:
●Chromebooks must have a Thousand Islands School District asset tag on them at all times and this tag must not be removed or altered in any way. If tag is removed disciplinary action will result.
●No food or drink is allowed next to your Chromebook while it is in use.
●Cords, cables, and removable storage devices must be inserted carefully into the Chromebook.
Never transport your Chromebook with the power cord plugged in. Never store your Chromebook in a case or backpack while plugged in.

●Students should never carry their Chromebooks while the screen is open.
●Chromebooks must remain free of any permanent writing, or drawing.
●Vents CANNOT be covered.
●Chromebooks should never be left in a car, unlocked locker, or any unsupervised area.
●Students are responsible for bringing completely charged Chromebooks for use each school day.

Taking Care of your Chromebook:
Students are responsible for the general care of the Chromebook they have been issued by the school. Chromebooks that are broken, or fail to work properly, must be submitted to the library of their school to be sent to the Help Desk as soon as possible so that they can be taken care of properly. Do not take district owned Chromebooks to an outside computer service for any type of repairs or maintenance.

Carrying Chromebooks:
●Transport Chromebooks with care.
●Chromebook lids should always be closed and tightly secured when moving.
●Never move a Chromebook by lifting from the screen. Always support a Chromebook from its bottom with lid closed.

Screen Care:
Chromebook screens can be easily damaged! The screens are particularly sensitive to damage from excessive pressure on the screen.

●Do not lean or put pressure on the top of the Chromebook when it is closed.
●Do not store the Chromebook with the screen in the open position.
●Do not place anything near the Chromebook that could put pressure on the screen.
●Do not place anything in a carrying case or backpack that will press against the cover.
●Do not poke the screen with anything that will mark or scratch the screen surface.
●Do not place anything on the keyboard before closing the lid (e.g. pens, pencils, or disks).
●Do not place the device near magnets or anything with high electric current.
●Clean the screen with a soft, dry microfiber cloth or anti-static cloth.

Using your Chromebook at school:
●Chromebooks are intended for use at school each day.
●In addition to teacher expectations for Chromebook use, school messages, announcements, calendars and schedules may be accessed using the Chromebook.
●Students are responsible for bringing their Chromebook to all classes, unless specifically advised not to do so by their class teacher.

Chromebooks Left at Home:
●If students leave their Chromebook at home, they will be allowed to phone their parent/guardian to bring it to school. This should occur before the school day starts or on lunch time to reduce distractions during the school day.
●If unable to contact parents or guardian to bring the device to school, the student can request a loaner from the library for the day.
●Repeat violations of this policy will result in disciplinary action.

Charging your Chromebook:
●Chromebooks must be brought to school each day fully charged.
●Students need to charge their Chromebooks each evening.

●Students grades 5 through 8 will have a charged Chromebook available at school each day unless policies change and allow for students to take them home. If/when this occurs then the aforementioned charging procedures apply.

Audio Restrictions:
●Sound must be muted at all times unless permission is obtained from the teacher for instructional purposes.
●Headphones may be used at the discretion of the teacher but may not be provided by the Thousand Islands School District.

Account Access:
●Students will only be able to log in using their *@tivikings.org email account.
●Access to personal google accounts will NOT be allowed on school issued devices.

Passwords:
●Take care to protect your password. Do not share your password.
●Password resets can be facilitated by staff. They will either reset it upon request or request to have it reset.

Internet safety:
●The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for Internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011. What CIPA requires Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an Internet safety policy that includes technology protection measures. The protection measures must block or filter Internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this Internet safety policy, schools and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal. Schools subject to CIPA have two additional certification requirements: 1) their Internet safety policies must include monitoring the online activities of minors; and 2) as required by the Protecting Children in the 21st Century Act, they must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. Schools and libraries subject to CIPA are required to adopt and implement an Internet safety policy addressing:
· Access by minors to inappropriate matter on the Internet.
· The safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications.
· Unauthorized access, including so-called “hacking,” and other unlawful activities by minors online;
· Unauthorized disclosure, use, and dissemination of personal information regarding minors; and
· Measures restricting minors' access to materials harmful to them. Schools and libraries must certify they are in compliance with CIPA before they can receive E-rate funding.
· CIPA does not apply to schools and libraries receiving discounts only for telecommunications service only.
· An authorized person may disable the blocking or filtering measure during use by an adult to enable access for bona fide research or other lawful purposes.
· CIPA does not require the tracking of Internet use by minors or adults.
You can find out more about CIPA or apply for E-rate funding by contacting the Universal Service Administrative Company's (USAC) Schools and Libraries Division (SLD) at www.sl.universalservice.org. SLD also operates a client service bureau to answer questions at 1-888-203-8100 or via email through the SLD website.

Web Filtering:
Thousand Islands has partnered with Securly to provide internet filtering for all student Google accounts and Chromebooks.

Who is Securly?
Securly is the leading provider of cloud-based web filters for schools and has a presence in thousands of schools across the US, Europe, and the Asia-Pacific region. Schools use Securly's web filter to maintain compliance with the Child Internet Protection Act, a federal law that mandates the use of Internet filters and other measures to protect children from explicit and inappropriate content.

What is Securly's Vision and Mission?
Securly's vision is to become a trusted household name among schools and parents for all aspects of a kid's online and offline safety.

Securly's mission is to create solutions that provide online safety to kids on both their school and personal devices. Securly strives to build features that allow schools and parents to work together to nurture and guide children in managing their screen time safely and productively.

Email Auditing:
Securly applies sentiment analysis to all email students send. The system automatically alerts staff of all messages related to bullying, self-harm, and profanity.

Securly Parent Portal:
Securly enables parents to engage in the online safety of their children. Parents/guardians will be able to monitor all internet activity for school-issued accounts/devices and receive weekly reports on their child's online activity.

●Thousand Islands requires a valid email for every parent wishing to partake in this service. Parents enrolled in our Schooltool parent portal will also gain access to the Securly parent portal. This service is available for students grades 6-12.

●To enroll in parent portal please go to our web site: http://www.1000islandsschools.org/parent-portal

24-hour monitoring:
Thousand Islands is committed to student safety and through Securly, we will leverage 24 hour monitoring of all student activity. Securly's team of student safety analysts will identify critical situations involving bullying, self-harm, or suicidal ideation. Securly will alert the district should any situation arise.

Personal Devices and TICSD accounts:
Thousand Islands accounts can be used on personal devices such as laptops, desktops, phones, and tablets. Please be aware that all activity done through the school account is tracked regardless of the device. All activity regardless of device is subject to this acceptable use agreement. Students are urged to log out of shared devices when not in use.

Acceptable use guidelines:
●The District Acceptable Use Policy applies to all student use of Chromebook devices.
●Students will have access to all available forms of electronic media and communication which is in support of education and research and in support of the educational goals and objectives of the Thousand Islands School District.
●Students are responsible for their ethical and educational use of the technology resources of the Thousand Islands School District.

●Access to the Thousand Islands School District technology resources is a privilege and not a right and can be revoked at any time.
●Transmission of any material that is in violation of any federal or state law is prohibited. This includes, but is not limited to the following: confidential information, copyrighted material, threatening or obscene material, and Chromebook viruses.
●Any attempt to alter data, the configuration of a Chromebook, or the files of another user, without the consent of the individual, building administrator, or technology administrator, will be considered an act of vandalism and subject to disciplinary action in accordance with the Acceptable Use Policy, student handbook and other applicable school policies.
●It is prohibited to take and/or distribute photos/videos/images with the knowledge and consent of the subject.

Privacy & Safety:
●Do not go into chat rooms or send chain letters without permission. If applicable, teachers may create discussion groups for communication among students for educational purposes.
●Do not open, use, or change files that do not belong to you.
●Do not reveal your full name, phone number, home address, social security number, credit card numbers, password or passwords of other people.
●Do not use your school email for personal email communication.
●Remember that storage is not guaranteed to be private or confidential as all Chromebook equipment and google accounts are the property of the Thousand Islands School District.
●If you inadvertently access a website that contains obscene, pornographic or otherwise offensive material, exit the site immediately.

Parent Responsibilities:
Parents are responsible for monitoring their student's use of the Chromebook at home and away from school. Parents are responsible for reviewing the TICSD Program Agreement with their child(ren)/student(s) and are asked to monitor their student's activities on the Internet on a regular basis.

Legal property:
●Comply with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a teacher or parent.
●Plagiarism is a violation of the student policy. Give credit to all sources used, whether quoted or summarized. This includes all forms of media on the Internet, such as graphics, movies, music, and text.
●Use or possession of hacking software is strictly prohibited and violators will be subject to discipline. Violation of applicable state or federal law, including the New York Penal Code, Computer Crimes, will result in criminal prosecution or disciplinary action by the Thousand Islands School District.

Google account:
Google accounts and access will be given to all students utilizing Chromebooks. This is a requirement that gives them access to sign into the device and participate in communication with peers and staff for educational use. Students under 13 ordinarily need parent permission to have gmail accounts, however COPPA allows the School District of Thousand Islands to act as the parent's' agent and approve the accounts on their behalf. To be COPPA (Children's Online Privacy Protection Act) compliant, we must provide an opt out process and have done that (see section 7e) so all students will have Google Apps accounts (including GMail) built into the private student domain.

E-mail electronic communication:
Google accounts and access will be given to all students utilizing Chromebooks. This is a requirement that gives them access to sign into the device and participate in communication with peers and staff for educational use. Always use appropriate and proper language in your communication.
●Do not transmit language / material that may be considered profane, obscene, abusive, or offensive to others.
●Do not send mass emails, chain letters or spam.

●E-mail & communications sent / received should be related to educational needs.
●E-mail & communications are subject to inspection by the school at any time.

Consequences:
●The student, in whose name a system account and/or Chromebook hardware is issued, will be responsible at all times for its appropriate use.
●Non-compliance with the policies of this document will result in disciplinary action.
●Electronic mail, network usage, and all stored files shall not be considered confidential and may be monitored at any time by designated district staff to ensure appropriate use.
●The district cooperates fully with local, state or federal officials in any investigation concerning or relating to violations of computer crime laws.

At Home Use:
●The use of Chromebooks at home is encouraged.
●School district-supplied filtering is active on each student account at all times.

Chromebooks left in Unsupervised Areas:
•Under no circumstances should Chromebooks be left in an unsupervised area or unattended.
•Unsupervised areas include the school grounds and campus, the cafeteria, computer labs, locker rooms, library, unlocked classrooms, music rooms and hallways.
•Any Chromebook left in these areas is in danger of being stolen.
•If an unsupervised Chromebook is found, notify a staff member immediately. Unsupervised Chromebooks will be confiscated by staff and taken to the Library/Office in the building. Disciplinary action may be taken for leaving your Chromebook in an unsupervised location.

Repairs and replacement for damaged and lost Chromebooks:
Middle School Chromebooks that need repair should be submitted to the classroom teacher. The classroom teacher will then submit a HelpDesk ticket to have the chromebook repaired. High School students should submit Chromebooks that need repair, to their building Library Staff. Library Staff should be notified of any damage or issue to a student's Chromebook

Chromebook Repairs:
●Chromebooks needing repair are to be turned in at the library or main office to have it repaired. All repairs will be managed by District IT Staff.
●Students and families should never attempt to fix a broken Chromebook nor should they have anyone else attempt to fix their Chromebook.
●Loaner device may be issued to students when their Chromebook is in for repair.
●Students using loaner device will be responsible for any damages incurred while in their possession.
●Students will be required to reimburse the District if a loaner device is lost or stolen.

Vendor Warranty:
●The vendor warrants the Chromebooks from defects in materials and workmanship.
●This limited warranty covers normal use, mechanical breakdown or faulty construction and will provide normal replacement parts necessary to repair the Chromebook or Chromebook replacement.
●The vendor warranty does not warrant against damage caused by misuse, abuse, accidents or Chromebook viruses.
●All vendor warranty claims will be handled by Technology Staff.

Chromebook Repair Costs:

Chromebook repair costs are determined below. Students and student families will be responsible for all damages to their District issued chromebook. If a device is lost or stolen the student and student family will be responsible to replace the chromebook. This includes chromebook chargers.
●Replace destroyed/Lost Chromebook- Cost for replacement will be based on depreciated value from time of purchase. All Chromebooks are depreciated over 4 years from time of purchase.

●Replacement Parts – TI will source replacement parts as cheaply as possible. Cost to family will determined at time of repair.

Chromebook technical support:

Technical support is available as follows. If repair is necessary for a Middle School Chromebook, then the classroom teacher must submit a technology request for repair. If repair is necessary for a High School Chromebook, then a Library Staff member will submit a technology request for repair.

Technology Staff members will provide:
●Hardware maintenance and repairs
●Password resets
●User account support
●Coordination and completion of warranty repairs

Library Staff can provide (High School Only):
●Charging of a chromebook, if deemed necessary and acceptable
●Loaning of a device
●Submission for repair

Thousand Islands CSD AUP & Chromebook Agreement Signature Sheet

The full policy can be found here: http://www.1000islandsschools.org/departments/technology

Student Agreement

The District's Acceptable Use Policy serves as official notification of acceptable use procedures for computer systems and district network access. Students wishing to utilize these technologies must agree to do so in a responsible, decent, ethical and polite manner. I have read, understand and agree to abide by the terms of the foregoing Acceptable Use Policy and Chromebook Program. I understand that this technology is designed for educational purposes. I understand and will abide by the Conditions, Rules and Acceptable Use Agreement. I also recognize that it is impossible for the Thousand Islands Central School District to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. Should I commit any violation or in any way misuse the school network or Chromebook, I understand and agree that my access privilege may be revoked and School disciplinary action may be taken against me. I understand that I am to treat all district own equipment with care. I will not alter, make changes to, or use district technology in any manner that is not aligned with the Acceptable Use Policy. If I am signing this Policy when I am under 18, I understand that when I turn 18, this Policy will continue to be in effect and I agree to abide by this Policy.

Student (print clearly) _____ Date _____

Student(signature) _____

Parent or Guardian Agreement

As the parent or legal guardian of the above minor, I have read, understand and agree that my child or ward shall comply with the terms of the Thousand Islands School District's Acceptable Use Policy and Chromebook Program. I understand that district technology resources are a privilege and can be revoked if misused. I understand that if district hardware is damaged, lost, or stolen that my child or myself will be responsible to reimburse the district for the cost of the repair or replacement. I am signing this Policy and agree to indemnify and hold harmless the School, and the School District that provides a device to my child or ward, against all claims, damages, losses and costs, of whatever kind, that may result from my child's or ward's use of his or her district hardware or violation of the foregoing Policy. Further, I accept full responsibility for supervision of my child's or ward's use of his or her Chromebook if and when such access is not in the School setting. I hereby give permission for my child or ward to use a Chromebook authorized by the School District and agree to the above terms and Policy.

Parent or Guardian (print clearly) _____ Date _____

Parent or Guardian (signature) _____