STUDENT ACCEPTABLE TECHNOLOGY USE POLICY (SATUP)

Purpose:

The purpose of this policy is to ensure that the use of Thompson School District (TSD) technology including hardware, software, communications (i.e, email, texting, chat, etc.), and network resources is consistent with Colorado and U.S. law and the district's objectives. Students that use district technology resources accessed from any location or device, including personal technology devices, are required to adhere to this policy. TSD reserves the right to modify terms and conditions at any time. The latest version is available from the district website at www.thompsonschools.org.

Introduction:

Students need the ability to use technology skillfully, wisely, and safely to be informed citizens, post secondary students, and/or future employees. As a fundamental part of their education, TSD provides access to district computers, communications systems, the Internet, student accounts, applications, and an array of other technology resources to promote educational excellence, innovation, and communication. Technology includes all district owned hardware, software, network access, and other related digital or physical resources and accessories. Technology integration in curriculum is a vital component of a quality education. Access to the Internet enables students to use learning management systems, digital curriculum, and extensive online libraries and databases. Online digital tools allow students to collaborate and share information electronically in ways that reflect how people work together in the real world and allows the district to teach digital citizenship and responsible use of technology.

In addition to curricular uses, technical systems are essential for school and district communications, enhanced productivity, and providing information to the local community, including parents, social service agencies, government agencies, and businesses.

The use of TSD technology should be used for educational purposes only. With access to information and people all over the world comes the possibility of accessing material that may not be considered educationally valuable in the context of teaching and learning. Therefore, the district has taken precautions to restrict access to inappropriate or offensive materials. Network firewalls, restrictions, and filters are in use that meet CIPA (*Children's Internet Protection Act*) mandates, but it's very difficult to control the quality of all materials that might be accessed. We firmly believe that the value of information and interaction available through the network far outweighs the possibility that users may encounter material that is not consistent with educational purposes.

Requirements:

This policy has different requirements depending on the type of technology. There are two categories of educational technology to consider. The first is *Required Curricular Technology*. This kind of technology is essential for the delivery of core academic content that a student must

learn to advance to the next grade or graduate from high school. Modern curriculum is infused with technology. Much of it is delivered online. So denying a student access to the needed technology would be tantamount to denying them equal access to the curriculum. **All technologies used for curricular purposes are required unless they are specifically listed in the optional Enhanced Technology category below. Technologies that are neither curricular or educationally enhancing in nature are prohibited.**

Some examples of required curricular technologies include the following:

- Centrally Managed Devices Issued to Students (i.e. iPads, Chromebooks & Laptops)
- Digital Curriculum and Textbooks (i.e. Science, Math, Social Studies, Language Arts)
- Learning Management Systems (i.e. Google Classroom, Seesaw, Blackboard)
- Subject Specific Practice Applications (i.e. mathematics drill & practice, language)
- Productivity and Organization Applications (i.e. word processor, calendar, presentation)
- Teacher-Student School Communications (i.e. email, video conferencing, gradebook)
- Internet Access (i.e. research, cloud storage, cloud-based applications)
- Behavior Management Systems (i.e. Securly Classroom, JAMF School)

The second category of educational technology is *Enhancing Technology*. This technology can improve the educational experience of classroom learning, clubs, or sports teams. Parents may opt their students out of this technology category, but doing so may prohibit their student from full participation in the affected activity. The following technologies are included in this category:

- Teacher-Parent-Student messaging applications
- Digital communication applications designed for team sports and/or clubs
- Sports performance analyzing and recruiting applications
- 3D printers and associated design software
- Physical education fitness monitors
- Assistive technology
- eSports gaming software

This policy contains guidelines to make students, parents/legal guardians aware of the expectations of students as responsible users of TSD technology. Student signatures (online or hard copy) at the end of this document or in association with online forms submitted with annual registration are representative of the signers' acknowledgement of their careful review of this policy and their knowing acceptance of these terms as a condition to their use of TSD technology. Students are expected to comply with the terms of this policy, as amended from time to time in the Board's absolute discretion.

<u>Proper and Acceptable Use of All Technology Resources:</u>

Users are expected to abide by the generally accepted rules of network and email etiquette and to conduct themselves in a responsible, ethical, and polite manner while utilizing technology. All district technology resources, including but not limited to, district computers, software,

communications systems (email, video conferencing, websites, cell phones, social media, text messaging, instant messaging, blogging, podcasting, email lists, and/or other emerging technologies) and the network, must be used in a manner consistent with the educational mission and objectives of TSD.

Student use of technology for activities that <u>are</u> permitted and encouraged include:

1. Completing school work;
2. Creating and presenting original academic work;
3. Researching topics being studied in school, opportunities outside of school related to community service, employment, or further education;
4. Publishing of student work online;
5. Engaging in distance learning experiences including video conferencing;
6. Completing online assessments;
7. Under district staff supervision, engaging in online collaborative educational projects using blogs, wikis, or other collaborative tools;
8. Under district staff supervision, engaging in electronic discussions with students, teachers, and experts outside the classroom;
9. Sharing or exchanging school-related files with students/teachers;
10. Completing online/Internet based college or financial aid applications using district technology resources;
11. Downloading educational videos, podcasts, or data;
12. Interacting with dynamic, adaptive, and/or simulated education content
13. Following District computer virus/malware protection procedures;
14. Following any individual school's or teacher's instruction for Internet use that may be imposed in addition to this policy.

Student activities that are <u>not</u> permitted when using district or personal technologies include but are not limited to:

1. Engaging in any illegal act or violation of any local, state, or federal statute or law;
2. Unauthorized access, modification, or encryption of any school district data;
3. Attempting and/or using Internet proxy servers for any purpose;
4. Possessing key logging or other monitoring devices, software, or malicious code;
5. Network monitoring or packet capturing;
6. Logging in or attempting to login as another user, with or without their consent or knowledge;
7. Purchasing apps or other online products using someone else's account or credentials;
8. Using a computer that is already logged in with someone else's credentials;
9. Computer vandalism, either physical or virtual;
10. Storing personal/non school related music and/or video collections on district file servers;
11. Loading unauthorized applications or software on district computers or other devices;
12. Attaching a wireless access point to the network or configuring a device (phone, laptop, etc.) to act as the same;
13. Configuring any district device to join an Internet bittorrent or other like system;

14. Enabling remote access to any district computer system without ITS staff permission;
15. Attempting to defeat district filtering software in any way;
16. Executing programs from removable media without prior approval by an authorized adult;
17. Violating copyright laws, including plagiarism and file downloads;
18. Accessing, reviewing, uploading, downloading, storing, printing, posting, transmitting, or distributing materials that
    - use language or images that are inappropriate in the educational setting or disruptive to the educational process or posting information or materials that could cause damage or danger of disruption;
    - are pornographic, obscene, or sexually explicit material;
    - use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination;
19. Knowingly or recklessly posting false or defamatory information about a person or organization or harassing another person or engaging in personal attacks, including prejudicial or discriminatory attacks;
20. Inciting violence or school disruption;
21. Using the network, video conferencing, or email in a way that disrupts the use of such technology by others. Abuse of resources is prohibited, such as the sending of annoying or unnecessary messages to a large number of people or other functions that might restrict or interrupt data flow;
22. Alteration of technology equipment setup, configuration, or intended use.
23. Sharing of passwords with unauthorized users, such as other students or third parties.

<u>Safety:</u>

As part of the district's dedication to providing a safe digital environment:

1. Students should not reveal personal information, such as passwords, home address, or phone number;
2. Students should not use their last name online unless it is part of a secure district provided account;
3. Students should not provide information that might allow another person to locate him or her unless the student has permission of a district employee to do so;
4. Students shall not arrange face-to-face meetings with persons (other than TSD staff) met on the Internet or through electronic communications;
5. Staff are not allowed to share personal student data such as full name and student number in unencrypted electronic communications. TSD domain Google email is encrypted.
6. Staff may use monitoring software on TSD accounts issued to students (i.e. Google Accounts) to ensure students are adhering to this policy and maintaining a safe focus on learning.

Students are expected to report harassment, threats, hate-speech, and inappropriate content to a teacher, counselor, or administrator. If a student has any questions about whether a specific activity is permitted, he or she should ask immediately.

Vandalism:

Any intentional act by a student that damages district technology including but not limited to hardware, software, operating systems, network systems, or data will be considered vandalism and will be subject to school rules, disciplinary procedures, restitution, and possible criminal prosecution. Any intentional act that requires repair or replacement of district technologies or data is also considered vandalism.

Limitations of Liability:

TSD makes no warranties of any kind, expressed or implied, for the technology resources it provides to students. TSD is not responsible for any damages suffered by the student, including those arising from non-deliveries, mis-deliveries, service interruptions, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies, is at the student's own risk. District use of Internet resources does not imply endorsement of content and/or advertisements. TSD specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. The student and his/her parent/guardian will indemnify and hold TSD harmless from any losses sustained as the result of use and/or misuse of the district's technology resources by the student.

Privacy:

Accounts issued to students (i.e. Google, Infinite Campus, Pearson Test Access) are not the property of the student. They belong to TSD and are issued to students while they are registered as students of the district for educational use only. TSD ensures compliance with the Colorado Student Data Transparency and Security Act. However, the privacy of TSD accounts issued to students is not guaranteed from within the TSD protected domain. When necessary, student accounts may be monitored by TSD or its agents for adherence to this policy. Although electronic communication and information is generally treated as private property, users on the district network do not have personal rights of privacy in anything they create, receive, send, or store on or through the network, on district computer systems, or through district- provided email accounts. Authorized personnel (which may include a student's parents or legal guardians) may review files and documents to maintain system integrity and ensure that users are using the system responsibly. The principal or designee also may review files, documents, email, or communication forums. Documents, files or emails related to or in support of illegal activities may be reported to the authorities.

Consequences:

Any violation of this policy may result in serious consequences including minor digital restriction, major digital restriction, account suspension, loss of computer privileges up to one year, dismissal from computer related classes, loss of all Internet/network and/or email access,

a temporary ban from computer labs, and/or other consequences imposed by school district policies and/or local, state or federal law, where applicable.

Guidelines and Regulations for Home Use and Loaned Technology:

These guidelines and procedures are necessary for each student and parent/guardian to understand and students to follow in order to help make the use of technology, and especially iPads/Chromebooks, safe and successful.

Home Use:

Outside of school, parents/guardians bear responsibility for the same supervision and guidance of students online as they exercise with other information sources such as television, telephones, radio, movies and other possibly offensive media. parents/guardians are responsible for monitoring their student's use of any district provided systems and/or electronic resources from home or another remote location.

While TSD does assist families in determining the best internet option for their situation, TSD does not guarantee internet access for home use. Parents are encouraged to review options for low income families found at

- www.xfinity.com/support/internet/comcast-broadband-opportunity-program
- www.centurylink.com/aboutus/community/community-development/lifeline.html

as affordable options for those that qualify. Since the district does not provide filtering for home use, parents/guardians are encouraged to set up their own parental controls on their own home networks. Parental controls can be configured on all major internet service providers such as

- www.xfinity.com/support/internet/set-up-parental-controls-with-comcast-networking
- https://internethelp.centurylink.com/internethelp/security-parental-controls.html.

Loaned Technology:

In some schools, technology will be loaned out to students for home use. When this occurs, the following guidelines apply.

A. Terms of Student Technology Loans

1. TSD will issue technology (i.e. iPads, cords, charging adapters, keyboards, Chromebooks) to students after they have registered or re-registered for school each school year and after they have signed this *Student Acceptable Technology Use Policy*.
2. TSD retains ownership of issued technology such as iPads, Chromebooks, or software.
3. Students may be subject to loss of privileges, disciplinary action, legal action and/or be financially responsible for the replacement cost of the loaned technology in the event of negligent or malicious damage and/or violation of the Acceptable Technology Use Policy.
4. A student's possession of district owned technology terminates upon withdrawal from TSD or no later than the last day of school, unless there is a reason for later/earlier termination as determined by the principal or district. At that time, all loaned devices,

cases, accessories, chargers, cords and other loaned technology must be returned to the school/district.

B. Damage, Loss, or Theft

The school covers the cost of reasonable repairs for accidental damages. Accidental damage is not negligent or malicious damage. If loaned technology is damaged, school administration will determine if it is accidental, negligent, or malicious damage. If a device is under warranty or insurance coverage, and damages are found to be accidental or due to normal wear and tear, the district will repair the damages under warranty/insurance. Any incidents of damage beyond accidental may become the responsibility of the student's family to pay for as a fine to cover the costs of repair. For example, damages to an iPad that was not in its case because a student removed the case would be deemed neglectful and subject to a repair fine.

The district does not cover the cost of loss, theft, negligence, and abuse of loaned equipment (i.e. iPad/Chromebook) and accessories. For example, throwing an iPad or using the iPad as an umbrella would be considered examples of neglect and abuse. If a device needs to be replaced due to loss, theft (out of school or unsupervised), neglect, or abuse, it is the family's financial responsibility to replace the device at the district's current replacement cost.

Decision chart in case of damage, loss, or theft:

Accidental* *Student accidentally broke or damaged equipment*	**Negligent**** *Student negligently damaged, broke, or lost equipment*	**Malicious**** *Student purposely damaged, broke, or stole equipment*
Incident #1 and #2 per school year = no fine Incident #3+ = raised to *Negligent* level and mandatory administration meeting with student. No school discipline consequences.	Fine issued into Student Information System and mandatory administration meeting with student (amount of fine depends on any repair/replacement costs). School discipline consequences are possible.	Fine issued into Student Information System and mandatory administration meeting with student (amount of fine depends on any repair or replacement costs). School discipline consequences are likely.

**TSD's iPad warranty covers manufacturer defects and breakage of iPads in cases. Chromebook insurance is optional for families to purchase and covers accidental damages. Wear and tear replacements are at no-cost and do not count as an accidental damage incident.*

***As determined by an investigation by school administration.*

The student or parent/ guardian is required to immediately notify a member of the school or technology support team in all cases of stolen or lost loaned equipment. The technology support team and administration may be able to assist in relocating the equipment if they are notified immediately.

1. *Parents/Guardians are responsible for filing a police report if loaned equipment was stolen from their student while the student was not at school or being directly supervised by school personnel.*
2. *Parents/Guardians are responsible for the replacement cost of a lost or stolen loaned equipment. The only exception to this rule is if the equipment was stolen while under the direct responsibility and supervision of a district staff member.*
3. *Students are advised to use their Google Drive account to backup their data to mitigate the consequences of lost or damaged hardware.*

C. Repossession
TSD reserves the right to repossess technology at any time.

D. Appropriation
All TSD issued equipment is the sole property of the school district. Any items not returned within 30 days of the last day of enrollment or the last day of the school year may be considered stolen property. Failure to return issued technology (such as iPads/Chromebooks and accessories) in a timely manner will be referred to law enforcement. If referred to law enforcement, stolen property charges may be filed.

E. Modification to the Program
TSD reserves the right to modify the terms of loaned technology use at any time.

F. Device Cases
Devices (i.e. iPads or Chromebooks) loaned to students with cases must be kept in a district-approved case at all times. Cases are provided for most loaned iPads and Chromebooks with charger and cord. These district-provided cases must be returned to the district in a similar condition to when they were issued upon return of the device, cord, and charger. Students are discouraged from drawing on device cases or putting stickers on them.

G. General Care of Loaned Technology
Technology in need of repair must be reported to a teacher or another member of the technology support team. General guidelines to follow:
1. Do not permanently alter the equipment in any way. This includes “jailbreaking.”
2. Charge loaned devices at night before school the next day.
3. Minimizing the number of photos and movies on a device will increase performance.
4. Backup your files on a regular basis to external storage such as Google Drive.
5. Do not write, draw, paint, place stickers or labels or otherwise deface loaned technology or its case.

6. Remember, loaned iPads/Chromebooks are the property of TSD and should always be left in a district-approved case if the device type has a fitted case available.
7. Never put weight, such as a pile of books, on a device like an iPad or Chromebook.
8. Liquids, food and other debris can damage devices. Avoid them while using technology.
9. Take care when inserting and removing cords to avoid damage to the ports and cables.
10. Do not expose technology to extreme temperatures, direct sunlight, or ultraviolet light for long or extended periods of time. Extreme heat or cold may cause damage. If the device has been in a cold or hot environment for a long period of time, let it reach room temperature before using it.
11. NEVER leave loaned technology outside or in a vehicle.

H. General Security

1. Never leave devices unsecured. Devices should be locked in a designated area or secured when not in use.
2. Students are expected to maintain the security of loaned technology, even during after-school activities. Unsupervised devices will be confiscated by staff, and disciplinary actions may be taken.
3. Each device has several identifying labels, including the district identification label (also known as the asset tag). Under no circumstances are you to modify, remove, or destroy these labels.

I. End of the Year Collection Procedure

Loaned Technology including cords, chargers, and cases will be returned on the date designated by the principal and the technology support team. If a student is leaving TSD, they will return all loaned technology and accessories on or before the date of withdrawal.

Annual Statement of Understanding
(this is also available through the online registration system)

Student: I understand and will abide by the Board policy JS concerning acceptable technology use. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be suspended or revoked, and may subject me to school disciplinary action and/or appropriate legal action may be taken. I acknowledge that the Board, in its discretion, can amend this policy at any time and that I have a continuing obligation to familiarize myself with these policy requirements, as hereafter amended.

Student User's **Full Name**:

_____

Grade or Graduation Yr. _____

Student User's **Signature**:

_____ Date: / /

Parent or Guardian: I hereby certify that I have read the Student Acceptable Technology Use Policy JS and discussed it with my student. I understand that use of technology in the Thompson School District is meant for educational purposes only. Thompson School District has taken precautions to eliminate inappropriate material, and students will not access unfiltered materials. I also recognize it is impossible for Thompson School District to restrict access to all inappropriate materials, and I will not hold the district responsible for materials acquired on the network nor will I hold the school district responsible for any financial obligations arising from unauthorized use of technology. Further, I accept full responsibility for my child's technology use when not in a school setting, or when using personal technology devices while on or near a school campus or during school transportation. I acknowledge that the Board, in its discretion, can amend this policy at any time and that I have a continuing obligation to familiarize myself with these policy requirements, as hereafter amended, and to discuss these with my child from time to time.

Parent or Guardian's **Full Name**: (Please Print):

_____

Parent or Guardian's **Signature** (If user is under 18 years of age):

_____ Date: / /

* If parents/guardians wish to opt their student out of using the second category of educational technology (Enhancing Technology), it is done so by separately writing to the student's school principal or the district's Chief Technology Officer.

Adopted September 2, 1998
Revised October 16, 2019
Revised February 3, 2021

LEGAL REFS.

20 U.S.C. 6751 *et seq. (Enhancing Education Through Technology Act of 2001)*
47 U.S.C. 254(h) *(Children's Internet Protection Act of 2000)*
47 C.F.R. Part 54, Subpart F *(Universal Support for Schools and Libraries)*
C.R.S. 22-87-101 *et seq. (Children's Internet Protection Act)*

CROSS REFS:

EGAEA, Electronic Communication
EHAA, Computer/Data Security
JKD/JKE, Suspension/Expulsion of Students