General

Unless otherwise specified, the following policies apply equally to all Twin Falls School District computing device and network users, including, but not limited to, students, guests, employees, volunteers, and contractors. Certain users may have additional rights, restrictions, or obligations due to the nature of their positions and/or access privileges.

Every student is required to have an agreement form signed and on file before the student will be allowed to use the computers or other networked devices.

All individuals with access to Twin Falls School District technology and data networks will:

- Respect the rights and property of others.
- Observe Twin Falls School District codes of conduct.
- Utilize the computers, network, Internet, and other technologies only for purposes supporting the District's stated educational goals or for legitimate School District business, unless otherwise allowed in policy.
- Take reasonable precautions to prevent loss or damage to equipment and data.
- Install and use software and hardware on the District's computers, other devices, and network only in accordance with this policy.

Interpretation, application, and modification of this use policy are within the sole discretion of the Twin Falls School District. Any questions or issues regarding this policy should be directed to District administration or the network administrator(s).

Computing Device and Network Use Rules

All District policies and rules pertaining to behavior and communication apply to computing device and network use. School District computing device users are expected to act in a responsible, ethical, and legal manner, in accordance with the missions and purposes of the District and the laws of the state and the United States.

Use of the computers, devices, and network is a privilege, not a right, and the privilege may be revoked at any time for unacceptable conduct. Unacceptable conduct includes, but is not limited to, the following:

- Using the computing devices or network for any illegal activity, including violation of copyright or other contracts.
- Using the computing devices or network for financial or commercial gain, including the development of Intellectual Property owned by the user.
- Using the computing devices for political or religious proselytizing or the promotion of opinions on elections, campaigns, or ballot issues in a way that presents such opinions as the view of the School District.

- Attempting to circumvent any security, content filtering, or traffic management measures implemented by the School District.
- Using the computing devices or network while access privileges are revoked or suspended.
- Gaining unauthorized access to resources or invading the privacy of an individual or organization.
- Vandalizing the data of an individual or organization.
- Misappropriating or plagiarizing data.
- Unauthorized downloading of software or media.
- Willfully and knowingly sending, accessing, or attempting to access obscene or other inappropriate material.
- Using an account owned by another user without authorization.
- Publicly posting personal communications without the author's consent.
- Placing unlawful or unlicensed information on a system.
- Using abusive, vulgar, or otherwise objectionable language in either public or private messages.
- Using the network, any Internet site, network service, or messaging system to harass, threaten, intimidate, or otherwise bully another individual.
- Using the network wastefully in a manner that would cause degradation or disruption of system performance, waste resources, or otherwise interfere with the productivity of others.

Network Etiquette and Conscientious Use

- Exercise caution with personally identifiable information. Do not reveal the personal information of others.
- Do not share your user account information with other individuals or leave your computer logged in unattended.
- Exercise caution with messages or files received from unknown senders or that seem suspicious.
- Use secure passwords and passphrases, and inform IT personnel if there is reason to believe an account has been accessed without authorization.
- Assume information accessible via the network and Internet to be private property and possibly copyrighted unless otherwise stated.
- Make backup copies of important files.
- Use broadcast messages only when they are work-related, and the content is important to all recipients.
- Adhere to applicable state and federal laws, including Family Educational Rights and Privacy Act and the Children's Online Privacy Protection Act, when posting and communicating.

Acceptable Posting

The Twin Falls School District provides a public Internet presence to share information with the community. Staff members are allowed to use these District provided resources and are responsible for monitoring and reviewing all content created by students. Students are not

allowed to directly publish information to any public School District sites. All posted information must comply with the Family Educational Rights and Privacy Act.

Users are prohibited from publishing, submitting, or displaying any information that:

- Violates copyright laws or property rights.
- Discloses student personal information other than names.
- Contains deliberately false or misleading statements regarding the School District, students, or staff.
- Is illegal.
- Is deliberately abusive, offensive, threatening, defamatory, or libelous.
- Is pornographic or otherwise obscene.

Social Media

Students are responsible for complying with School District policies and procedures when posting content on social media sites or other Internet sites when using the School District computing devices, network, or software and/or while in attendance at school. Student posts on social media sites or other Internet sites outside of school hours and school grounds using a personal device shall be private as long as they do not disrupt the School District's learning atmosphere, educational programs, or activities, or otherwise interfere with the orderly operation of the school or the rights of others. Posts to social network sites using a District computing device, network, or software may be subject to public records requests.

Staff members are expected to comply with the Employee Use of Social Media Sites policies.

False Entry/Alterations

No student, volunteer, or School District employee will make any false entry or alteration of any document, either paper or electronic, used or intended to be used in connection with the operation of the Twin Falls School District, nor will any student access or alter official school documents or private documents, either paper or electronic.

Copyrighted Material

Copyrighted material will not be placed on any system connected to the District's network without the author's permission. Only the owner(s) or persons specifically authorized may upload copyrighted material to the network. Users may download only that copyrighted material for which permission has been requested and granted, or that falls within the fair use exception to the copyright laws. A user may redistribute copyrighted programs, materials, or media only with the express permission of the owner or authorized person or as provided by the fair use exception.

Controlled Access to the Internet

Internet access is provided for use consistent with the District's educational and business goals. It is the practice of the Twin Falls School District to make a reasonable effort to prevent exposure of staff and students to obscene, pornographic, and other inappropriate material available on the Internet by monitoring Internet access and by using technological mechanisms

such as content filters and firewalls in accordance with the Children's Internet Protection Act. Students accessing the Internet at school, regardless of whether on School District devices or on student-owned devices are required to connect to the Internet through the District's content filter. Despite these efforts, users may encounter information on the Internet that is controversial or potentially harmful. Because information and locations of information are continually changing, it is impossible for the District to monitor all content. Some computer systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal materials. The District does not condone the use of such materials and does not knowingly permit use of such materials. Known attempts to access inappropriate material are logged, and deliberate attempts to access obscene or inappropriate materials or to circumvent content filters and firewalls by any user will result in disciplinary action by School District administration. While using the Internet, any student receiving unsolicited requests for personal information is required to immediately report the request to the supervising teacher. To help students be conscientious Internet users, the District includes a component of Internet safety in the District's instructional program, with topics including appropriate online social interaction.

Unlawful and Unauthorized Activities

The Twin Falls School District prohibits the use of the network or computing devices for illegal activities, including electronic crimes such as unauthorized access, deliberate use of malicious code such as viruses or malware, and deliberate attacks on systems ("hacking"). These activities will result in disciplinary action by School District administration.

Security

Attempts to log onto the network with another person's identification without permission may result in disciplinary action. Students are prohibited from using any account belonging to a staff member. Any user identified as a security risk or having a history of problems with other computer systems or networks may be denied access to the District computing devices and network. Any user who feels that he or she can identify a security problem or data breach on the network must immediately notify an administrator and not demonstrate the problem to others.

User Privacy

No user of the School District computing equipment or network has a reasonable expectation of privacy in such use. Administrative or IT personnel may audit, monitor, or review the use of the equipment and network periodically or for a specific cause. IT personnel may see e-mail messages and files during operational procedures or troubleshooting. All works created or stored by a user on the computers, network, or storage devices are subject to the monitoring and scrutiny of District administration, designated IT personnel, or other designees of administrators.

User Accounts

Network users may be issued individual user accounts to log on to the District network and access services, including District email and other information systems. Individual student accounts will be issued and revoked as deemed necessary by administrative and IT personnel. For staff, District administration will determine if an account for a specific information system is

necessary for each employee position. Substitute employees, temporary employees, and volunteers will typically not be issued accounts. In certain cases, long-term substitute employees may be issued accounts if deemed necessary by administration. District IT personnel will make a reasonable effort to retain an employee's email access for thirty (30) days following that employee's resignation, after which all account access and system privileges will cease. System and network access for terminated employees will cease immediately. An account that is inactive for more than thirty (30) days may be removed along with that user's files without notice given to the user. Any employee taking a leave of absence must contact the IT department prior to the absence to request that his or her account(s) and/or files not be removed. IT personnel and District administration are empowered to suspend some or all privileges associated with computing device use and network access for any user in cases of suspected misuse, suspected threat to the integrity of information technology resources, or suspected misconduct of any kind. All files, materials, or documents stored on District devices or servers may be reviewed by and may be deleted by designated IT personnel.

Intellectual Property

All works of any kind that an employee of the School District creates on District computing devices or network shall be the intellectual property of the School District, as such property shall be deemed "work for hire" as defined in 17 U.S.C. Section 1001(1).

Email

The School District may provide email accounts for staff and students to conduct School District business or as a tool for accomplishing the District's education goals. IT system administrators may see the contents of email messages in the process of system maintenance, investigation, or troubleshooting, but will not intentionally inspect the contents or disclose the contents to anyone other than the sender or intended recipient without the consent of the sender or intended recipient, except in accordance with state or federal law or District policy. Cancelled network accounts do not retain their email. Individual messages cannot be recovered once deleted. To conserve resources, IT personnel may set quota restrictions and time limits on storage, and system administrators may remove email messages if not attended to regularly by the users. The District does not employ an automated email archiving system; therefore users are expected to be aware of the statutory and legal obligations related to the information which they are storing, to retain records for the appropriate period of time, and to not conduct non-District business on District messaging systems.

E-mail can be used to communicate with parents and students; however, e-mail sent and received from outside the School District e-mail system is not encrypted and should not be considered secure from unauthorized interception. Staff should not use personal identifiers such as student names or numbers in e-mail subject lines and should avoid sending personally identifiable confidential information.

District records, including e-mail, are subject to public records requests and disclosure to law enforcement, government officials, or other third parties through subpoena or other processes. District administrators may review any and all e-mail or Internet records of any employee, at any

time, with or without cause. Consequently, employees should ensure that information contained in e-mail and Internet messages is appropriate and lawful.

Violations and Enforcement

Violation of the rules set forth by School District policy may result in disciplinary action by School District administration. School District administration and IT system managers will make all decisions regarding whether or not a user has violated this policy and any related rules or regulations and may deny, revoke, or suspend access at any time, with his/her/their decision being final. Before any permanent action is taken against a user, the user will be advised of the basis for the proposed action and given an opportunity to respond. The specific disciplinary action for each case will be at the sole discretion of School District administration and may vary depending on the severity of the infraction. A student may lose computing device privileges and network access as a result of violating this policy. The duration of the loss will depend on the student's age and severity of the violation as determined by District administration and the IT system administrator(s). Students found to flagrantly or persistently violate this policy may lose all privileges for the remainder of the school year or for the duration of school attendance. A student may be removed from class, suspended, or expelled from school if he or she engages in conduct on the computer network that constitutes a flagrant or persistent violation of this policy or could be considered illegal, as defined by federal or state law. Students committing illegal acts may be referred to the appropriate law enforcement agency. Each student is responsible for any damage he or she may cause to the District's computing devices, network, and/or data. The student must pay all costs incurred in restoring the computing devices, network, and/or data to its previous working order. A staff member may lose computing device privileges and network access as a result of violating this policy. The duration of loss will depend on the severity of the violation as determined by District administration and IT system administrators. A staff member may be disciplined, up to and including termination from employment, if he or she engages in conduct on the computing devices or network that constitutes a flagrant or persistent violation of this policy or could be considered illegal, as defined by federal or state law. Staff members committing illegal acts will be referred to the appropriate law enforcement agency.

Software Policy and Procedures

Purpose

Twin Falls School District licenses software applications from a variety of third parties for use on computers and other computing devices. Software developers generally copyright such software. Unless expressly authorized to do so, the Twin Falls School District has no right to make copies of the software except for legal backup or archival purposes. The purpose of this policy is to prevent copyright infringement and unlawful software use and to protect the integrity of the School District's computing device environment from viruses, malware, and similar threats.

Licensing Compliance

It is the policy of Twin Falls School District to respect all computing device software copyrights and to adhere to the terms of all software licenses to which the District is a party. School District

employees, students, or other users may not duplicate any licensed software or related documentation for use either on school premises or elsewhere unless expressly authorized to do so by agreement with the licenser. Unauthorized duplication of software may subject employees, students, and/or the District to both civil and criminal penalties under copyright laws. Employees may not give licensed District software to any other employee or non-employees, including parents, contractors, students, and others. School District employees and students may use software on networks or on multiple machines only in accordance with applicable license agreements. Students will not install computer software or tamper in any way with District software unless under direct supervision of a staff member and only with approved software. Anyone bringing media or downloading files from home or other outside sources is responsible to ensure that the content is legal and free from viruses and malware.

Use on Non-District Computing Devices

The School District's computing devices are District assets and must be kept both software legal and malware free. Only software acquired through the procedures outlined in this policy may be used on District computers. Generally, District owned software cannot be installed on non-District owned computing devices. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. Before taking any software home or off-site, users must check with the school software manager and follow sign-out and sign-in procedures.

Acquisition of Stand-Alone Software

To purchase and utilize software on the computers or network within the School District, each user must obtain the approval of his or her District IT department technician to ensure compatibility with District systems. All software may be subject to review and approval by the Twin Falls School District Curriculum Committee or the IT Department.

Acquisition of District-Wide Software

In order to facilitate the selection and implementation of software for use District-wide, an evaluation committee of District staff will be assembled to analyze and evaluate software packages or services under consideration. The committee participants will include a representation of stakeholders and be led by a project manager assigned by District administration to ensure that the selection best meets the needs of the District. At all stages, factors such as user reaction, impact on the workload and efficiency of users and support personnel, and resources required should be considered. The committee will evaluate the need and justification for the software, the feasibility, and alternative options. All necessary components, including software, hardware, training, and ongoing costs will be considered.

Software Audits

District IT personnel may conduct random audits of all District computing devices to ensure that the District is in compliance with software licenses. During these random audits the District personnel will eliminate any inappropriate software that is found.

Hardware Policy and Procedures

Property Rights

The Twin Falls School District has the right to specify who uses its equipment and the information contained therein, under what circumstances, and to what purpose. Equipment purchased or received by way of a grant award to a staff member, school, or the District is the property of the District. District and school administration will determine the use. Employees, volunteers, students, or other users do not have ownership rights to any equipment loaned to them by the School District. Any devices issued to employees are to be used, almost exclusively, for School District related purposes. Use of District equipment and software for private or personal business gain is strictly prohibited and will subject the violator to disciplinary action. No person will have exclusive use of District equipment unless authorized by District administration. School District-issued devices may be equipped with the ability to be accessed remotely at any time by IT personnel for technical support, tracking of missing or stolen devices, or any other appropriate purpose. Any individual in receipt of a School District-issued device does not have the authority to deactivate the remote access feature of the device. District-issued equipment is to be surrendered back to the School District immediately upon request.

Care and Safety

Employees, students, or others in receipt of District-issued equipment shall be held responsible for the safekeeping of the equipment and exercise reasonable efforts to see that the equipment is not lost, stolen, or damaged. As devices issued to employees may have access to privileged information such as staff and student data or student-restricted Internet sites, employees are expected to use password protection or similar security measures on their District-issued devices and to keep their passwords confidential, except for requested disclosure by school administration or IT personnel. Under no circumstances should devices be left in unsupervised areas, including, but not limited to, cafeterias, open computer labs, locker rooms, libraries, unlocked classrooms, dressing rooms, and hallways. Reckless or irresponsible use of School District equipment resulting in loss or damage may result in the user being required to reimburse the District for any associated costs of replacement or repair.

Use of Devices off School District Premises

District or building administration may permit certain devices to be used by staff or students off School District grounds. Before students are allowed to take District-owned device off school premises, each student must have completed both a Mobile Computing Device Use Agreement and a Computing Device and Network Acceptable Use Agreement on file at his or her school. Each form must be signed by the student and by a parent or guardian, if the student is less than eighteen years of age. A student's parent or guardian may be required to attend an orientation meeting and may be required to purchase insurance before a student is allowed to take devices off School District property. Students may only take the devices out of the State of Idaho with the explicit permission of school administration.

Parents or guardians of students may use school-issued devices to assist their child with learning, however use of school-issued technology outside of this purpose, such as for personal gain or

activities unrelated to student learning, is prohibited. Both parent and student use of the District's devices, network, and/or software applications may be subject to remote monitoring and/or public records requests. Content filtering may be utilized on District-owned devices that are used off school grounds, and any individual in receipt of a School District-issued device does not have the authority to deactivate the content filtering features or security features of the device.

Devices issued to students are intended for use at school each day. Students are responsible for bringing their device to all classes, unless specifically advised not to do so by their teacher. Devices must be brought to school each day in a fully charged condition, and necessary power cords must stay with the device at all times. Repeated failures to comply with these requirements may result in disciplinary action.

Individually Issued Devices

Staff and students that are issued individual devices are expected to use password protection or similar security measures on their District-issued devices and to keep their passwords confidential, except for requested disclosure by school administration or IT personnel.

Using stickers, drawings, permanent markers, or in any other way defacing or modifying device hardware is not allowed, and may result in disciplinary action.

Staff and students may place individualized items on individually issued devices, which are limited to music, pictures, and other items that do not hinder the network or device functionality. Staff and students may be permitted to select their own screen savers and backgrounds, provided they are appropriate. Use of screensavers, backgrounds, or other pictures containing guns, weapons, pornographic materials, inappropriate language, alcohol, drugs, gang-related symbols or images, or other items deemed inappropriate by the administration may result in disciplinary action. Students may not add options or upgrades to the device, change the operating system, or add unauthorized software. Should students or parents/guardians place personalized items on a device, such items may be accessed or viewed by District staff at any time, for any reason, including randomly selected device reviews. No content placed on District provided devices is privileged or confidential.

The software originally installed by the school must remain on the devices in usable condition and be easily accessible at all times. From time to time, the school may add, update, or remove software applications. The licensing for some software applications may require that the software be deleted from devices at the completion of a course, and periodic reviews of devices may be made to ensure that students have deleted software that is no longer required. It is the responsibility of individual students to be aware of the software applications and files which are required for classes and/or school activities. Additional software applications added by students must be appropriate for the school environment and comply with District policy. Violent or inappropriate games are banned from being installed on District-owned devices. The determination of whether a game is violent or inappropriate will be made by the teacher and school administration. Each student is responsible for ensuring that only licensed software and legally obtained media files are loaded on his or her device.

Students and staff are to report all device problems as soon as possible to District IT personnel or school administration.

The schools will utilize procedures for the maintenance of records regarding the devices, including tracking device inventory. At the end of the school year, the school will collect all devices from students. At the school's discretion, students may be issued devices to support summer school programs.

Acquisition of Devices

Before acquiring any new computing devices, computer-related equipment, or networked devices, each employee must consult with his or her District IT personnel to ensure compatibility with the District's computing and network platforms.

Wireless Devices

Use of wireless equipment on any District network other than the guest wireless network must be approved by the building IT personnel to ensure the compatibility, stability, and security of the District network. To ensure that security standards are met, wireless devices will not be used until configured appropriately by District IT personnel. Any wireless device deemed to be a security risk will not be allowed. Scans for rogue wireless devices may be performed by District IT personnel.

Non-District Owned Devices and Guest Network Access

Guest wireless Internet access may be available in some locations for visitor, staff, and student personal device use. Students are required to have an agreement form signed and on file before the student will be allowed to use non-District owned devices on the guest network. Users of the guest network should have no service level expectations, as there will be no technical support for personal devices and no guarantees of uptime, bandwidth availability, or access to any specific feature or service. Use of the guest network is a revocable privilege.

Student-Owned Devices (BYOD)

Students are prohibited from using electronic communication and entertainment devices on school grounds during school hours, unless expressly authorized to do so by school administration or if an emergency situation exists that involves imminent physical danger. The times and areas in which devices can be used will be determined by building administration.

School District policies pertaining to student conduct apply to the use of electronic devices. Students who use electronic devices for illegal or unethical purposes, including, but not limited to, cheating and harassment, could face suspension and/or expulsion, could lose the privilege of having electronics on school grounds, and, in the case of illegal activities, will be referred to the appropriate law enforcement agency.

As a privilege, students may be allowed to use student-owned devices to supplement the education process, though will not be expected or required to provide their own devices for any

purpose. Students are required to have an acceptable use agreement form signed and on file before the student will be allowed to use non-District owned devices during school, and the rules and guidelines of this acceptable use policy apply to student owned devices. If such devices are used, there will be no expectation by the student for technical support or access to District resources, including, but not limited to, District wireless or wired networks and District-owned software or applications. The School District cannot be responsible for content accessed via the student's voice, messaging, or data services. The District will not pay for or reimburse for any voice, messaging, or data charges incurred by a student's use of his or her own device. The School District does not assume liability in the event of lost, stolen, or damaged devices.

Camera use may be allowed in school when schoolwork requires it. Permission must be obtained from the subject of any photograph taken by a student-owned device, and permission must be obtained prior to any public distribution of a photograph. Use of any camera in locker rooms, restrooms, or other areas where there is an expectation of privacy is strictly prohibited and will result in suspension, expulsion, other disciplinary action, and/or referral to the appropriate law enforcement agency.

Staff-Owned Devices (BYOD)

Staff members are allowed to carry and use personal devices during work hours, however if such devices are used, there will be no expectation by staff members for technical support or access to District resources, including, but not limited to, District wireless or wired networks and District-owned software or applications. The District will not pay for or reimburse for any voice, messaging, or data charges incurred by a staff member's use of his or her own device. Personally owned devices should not be used during the employee's normal duty times, unless being used for the purpose of one's District job duties. Personal use is allowable during normal break times, lunch times, and preparation times.

Warranties and Indemnification

The School District makes no warranties of any kind, express or implied, in connection with its provision of access to and use of its voice and data networks and the Internet provided under this policy. IT personnel reserve the right to set restrictions and time limits on storage and bandwidth. The network services provided by the School District may not always meet student or staff requirements or be uninterrupted or error-free. The District is not responsible for any information that may be lost, damaged, or unavailable when using the network, or for any information that is retrieved or transmitted via the Internet. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Users are responsible for backing up their data. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services. The District will not be responsible for any unauthorized charges or fees resulting from access to the Internet, and any user is fully responsible to the District and shall indemnify and hold the District, its trustees, administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from such user's access to its computer network and the Internet, including, but not limited to, any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or legal guardian(s) agrees to

cooperate with the District in the event of the school's initiating an investigation of a user's use of his or her access to its computer network and the Internet. The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.

This policy shall be filed with the State Superintendent of Public Instruction every five (5) years after initial submission and subsequent to any edit to this policy thereafter. The Superintendent shall promulgate procedures to enforce this policy and to handle complaints about such enforcement. These procedures shall be available for review at the District office.

DEFINITION:
"Electronic communication and entertainment devices" shall include, but not be limited to, personal cell phones, smartphones, MP3 players, notebook computers, computer tablets, and other similar devices or media players, without regard to the commercial name or manufacturer of the device.

♦ ♦ ♦ ♦ ♦ ♦ ♦

Legal Reference: 17 U.S.C. Section 1001
Children's Internet Protection Act, Sections 1703 to 1721, U.S.C. Section 254(h)(1)
Idaho Code Sections 6-210, 18-917A, 18-1507, 18-1514, 18-2201, 18-2202, 33-132

Policy History:

ADOPTED: 5/2001

REVISED: 4/2014
8/11/14
8/10/15

School district computing device and network users are expected to act in a responsible, ethical, and legal manner, in accordance with district policy and the laws of the State of Idaho and the United States. The devices and network are provided to further the district's stated educational goals, and they are to be used by authorized individuals only. Individuals using these systems are subject to having all activities monitored by IT or other security personnel. Anyone using these systems expressly consents to such monitoring.

It is possible for all users of the internet, including your child, to access information that is not intended for minors. Although the district has taken reasonable steps to ensure that the internet connection is used only for purposes consistent with the curriculum and that inappropriate sites as defined by the Children's Internet Protection Act (CIPA) are filtered, the district or school cannot entirely prevent the availability of inappropriate material on the internet. Further, it is possible that a determined user may make use of computing devices or network resources for inappropriate purposes. Deliberate misuse of the computing devices, the network, or the internet may result in disciplinary action as outlined in the Computing Device and Network Acceptable Use Policy.

Curriculum for students will include instruction on internet safety topics, including appropriate online social interaction. Students are expected to use good judgment and follow the guidelines of the Computing Device and Network Acceptable Use Policy.

With school administration and teacher approval, your child may be allowed to use, but will not be required to use, his or her own electronic devices during class time for educational purposes. The school district cannot be responsible for the content accessed via a student's own voice, messaging, or data services. The district will not pay for or reimburse for any voice, messaging, or data charges incurred by a student's use of his or her own device. The school district does not assume liability in the event of lost, stolen, or damaged devices.

Please Check One

☐ Yes, my child may use his or her own electronic devices at school.

☐ No, my child may not use his or her own electronic devices at school.

I have discussed the information contained in the Computing Device and Network Acceptable Use Policy with my child. Should my child breach the policy guidelines, I understand that my child may lose privileges relating to the use of computing devices and the internet or be subject to other disciplinary action. I agree to indemnify and hold harmless the school district, the trustees, administrators, teachers and other staff against all claims, damages, losses, and costs, of whatever kind, that may result from my child's use of his or her access to such networks or his or her violation of district policy. Further, I accept full responsibility for supervision of my child's use of user accounts and the use of district-owned devices when such use is not in the school setting. I give my child permission to use district provided user accounts to access the district's data network and the internet.

_____	_____
Parent or Guardian Name (please print)	Student Name (please print)
_____	_____
Parent or Guardian Signature	Student Signature
_____	_____
Date	Date

This agreement is required for students who are individually assigned district-owned computing devices.

This agreement is valid for the 20xx-20xx school year.

STUDENT

- I understand and agree to the terms of the Computing Device and Network Acceptable Use Policy. Should any policy violation or misuse of the district-owned device occur while it is in my custody, I understand that I may lose the privilege of the device out of the classroom, may lose access to it entirely, or may face other disciplinary action.
- I accept full responsibility for the secure handling and safeguarding of the district-owned device. I understand that it is my responsibility to immediately report any damage, theft, or problems with the device to a teacher or school administrator.

Student First Name: _____ Last Name: _____ Phone: _____

Student Signature: _____ Date: _____

Physical Address (Street, City, Zip Code): _____

PARENT/LEGAL GUARDIAN

If the student is under 18 years of age, a parent or other legal guardian must complete the section below.

- I have read the Computing Device and Network Acceptable Use Policy and explained it to my child. If any policy violation or misuse of a district-owned device occurs while it is in my child's custody, I understand that my child's access to the device may be limited, suspended, or terminated, and that my child may face other disciplinary action.
- I understand that my child is responsible for the secure handling and safeguarding of the district-owned device. I understand that if my child is found to have deliberately or negligently damaged or lost the device, I will be financially responsible for reasonable repair or replacement costs.
- I understand that I will be responsible for monitoring my child's use of the device outside the school setting.

Please Check One

☐ My child is allowed to take assigned district-owned devices off the school campus.

OR

☐ I **do not** want my child to take assigned devices off the school campus.

Parent/Legal Guardian Full Name: _____ Phone: _____

Parent/Legal Guardian Signature: _____ Date: _____

Physical Address (Street, City, Zip Code): _____