



**Summit Public Schools:
Internet and Device Acceptable Use policy
(Students/Parents)**

[A. INTRODUCTION](#)

[B. GENERAL PRINCIPLES OF ACCESS](#)

[C. TECHNOLOGY TEAM RESPONSIBILITIES](#)

[D. LIMITATION OF LIABILITY](#)

[E. CONTENT FILTERING](#)

[F. REGULATIONS OF ACCESS](#)

[1\) Important Consequences of Access](#)

[2\) Privacy](#)

[3\) Parental Notification and Responsibility](#)

[4\) Access](#)

[5\) Limitations on Internet Usage](#)

[G\) E-mail Policy](#)

[H\) Device Use](#)

[I\) Bring Your Own Device \(BYOD\)](#)

[J\) Cyberbullying](#)

[K\) Cyber Incidents](#)

A. INTRODUCTION

Welcome to the document that explains our electronic policy!

Although this is a long and detailed policy, it is very important that you read it thoroughly because it explains everything you need to know about using the Internet, computers and other devices at a Summit school. It is your responsibility to use the Internet in ways that follow and support this policy.

All electronic usage throughout the Summit schools, including the things you do on a day to day basis, will be governed by this policy document. Your use - or misuse - of any electronics while at school will be interpreted according to this policy.

If you have any questions about the expectations set out in this document, please contact the Executive Director and or school administrator of your school site.

B. GENERAL PRINCIPLES OF ACCESS

Summit Public Schools (SPS) provides access to the Internet, including access to e-mail, for its schools, faculties, students, and guests. Guests include but are not limited to parents, student teachers, temporary employees, parent volunteers, and other school volunteers. All Internet access, including the use of e-mail, occurs through SPS's system.

This Internet and Device Acceptable Use Policy governs all electronic activity, including e-mail and access to the Internet, which is undertaken by SPS faculties, students, and parents/guardians either in their official SPS capacity or as part of the educational, instructional or extracurricular programs connected to the SPS. No SPS faculty member, student, guest or parent/guardian may engage in activities prohibited by this policy, whether through the SPS's Internet service or through any other Internet Service Provider, for whatever reason. Parents are strongly encouraged to discuss and monitor their child's school Internet use and to discuss any issues or concerns that they may have with the school's teacher and administrators. All use of the Internet will be governed by this policy.

C. TECHNOLOGY TEAM RESPONSIBILITIES

- 1) The Chief Technology Officer, or his/her designee, will serve as the coordinator to oversee Internet access on SPS systems.
- 2) The Executive Director and designated administrators of each school are responsible for the dissemination of this Internet and Device Acceptable Use Policy and they will work to enforce this policy on their site.
- 3) SPS reserves the right to revise this Internet and Device Acceptable Use Policy as it deems necessary. The most current policy will be linked through the Family Handbook.

D. LIMITATION OF LIABILITY

- 1) SPS makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the SPS system will be error-free or without defect. SPS will not be responsible for

any damage users may suffer, including but not limited to, loss of data or interruptions of service. SPS is not responsible for the accuracy or quality of the information obtained through or stored on the system. SPS will not be responsible for financial obligations arising from a user's unauthorized use of the system.

2) Users will indemnify and hold SPS and its respective schools harmless from any losses sustained by SPS as a result of intentional misuse of the system by user.

E. CONTENT FILTERING

SPS has installed Internet filtering software in a best-effort attempt to block user access to inappropriate and/or harmful content on the Internet. No filtering technology is perfect, and this technology may occasionally fail. In the event that the filtering software is unsuccessful and students gain access to inappropriate and/or harmful material, SPS and individual school sites will not be liable.

SPS filtering systems adhere to the US Congress enacted CIPA (Children's Internet Protection Act) guidelines, updated 2017: <http://www.fcc.gov/guides/childrens-internet-protection-act>

The filter is set at the most restrictive setting in restricting access to Internet sites that may contain interactive chat or mail or information regarding:

- Sex acts
- Sex attire
- Sex/nudity
- Sex/personal
- Basic sex education
- Advanced sex education
- Sexuality
- Sports
- Gambling
- Pornography
- Hacking
- Proxy avoidance
- Addictions
- Forums
- Social Networks
- Violence
- Streaming Music
- Non Academic Videos
- Illegal Drugs
- Weapons
- Criminal Activity
- Chat
- Torrenting
- Hate and Intolerance

F. REGULATIONS OF ACCESS

1) Important Consequences of Access

- a) SPS will always cooperate fully with local, state, or federal officials in any lawful investigation concerning or relating to any illegal activities conducted through the SPS system.
- b) Internet access is a privilege, not a right, and all students should be aware that SPS may revoke Internet access for any reason. If a student's access is revoked, SPS will provide an explanation for the revocation and the school site will ensure that the student continues to have equal access to participate in the educational program.
- c) It is very important for students and families to understand that violations of this Internet and Device Acceptable Use Policy DO count as disciplinary actions. All violations of this policy will be addressed according to the graduated discipline plan of the school that the student attends. Students and their families WILL have to meet specific concerns related to the violation and cooperate with the school to help the student acquire the specific behaviors necessary to behave appropriately on an electronic network.

2) Privacy

Users of the SPS system should understand that there is no expectation of privacy on this system.

- a) SPS reserves the right to monitor the use of the Internet through its system, at all times. SPS will collect and store information about usage which includes, but may not be limited to, the date and time a user visits the site and information about the user's activities while online. Except as otherwise specified in this Internet and Device Acceptable Use Policy, SPS will not use cookies to gather personal identifying information about any of its users (cookies are computer programs that store information about a user on a computer hard drive or disk and allow SPS, among other things, to verify whether a visitor is an authorized user of the SPS system.) Personal identifying information includes, but is not limited to, names, home addresses, e-mail addresses and telephone numbers.
- b) As required by the Children's Internet Protection Act ("CIPA"), SPS will monitor students' online activities. Such monitoring may lead to discovery that the user has violated or may be violating, SPS Internet and Device Acceptable Use Policy, the student handbook, or the law. SPS also reserves the right to monitor other users (e.g., non students) online activities.
- c) SPS reserves the right to employ and review the results of software that searches, monitors and/or identifies potential violations of the Internet and Device Acceptable Use Policy.
- d) Users should be aware that their personal files may be discoverable in court and administrative proceedings and in accordance with public records laws.
- e) System users should have no privacy expectation in the contents of their personal files and records of their online activity while on the SPS system. SPS does not encourage users to store personal data on the SPS system - SPS cannot be responsible for the loss or damage of such data.
- f) SPS may collect and store information about usage which includes, but is not limited to, the date and time a user visits a website and information about the user's activities while online. In addition, SPS students may access online platforms such as YouTube and Google Maps (complete list here), and these online platforms may collect and use your child's personal information. By utilizing SPS technology, you consent to this collection and usage.

3) Parental Notification and Responsibility

a) Where appropriate, individual schools will provide students and parents with guidelines and instructions for student safety while using the Internet.

b) SPS Internet and Device Acceptable Use Policy contains restrictions on accessing inappropriate material. However, there is a wide range of material available on the Internet, some of which may or may not fit the particular values of students and families. While student internet use will be logged, it is not practically possible for SPS to monitor and enforce a wide range of social values in student use of the Internet. Further, SPS recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. SPS strongly encourages parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through SPS system.

4) Access

a) Students will generally be provided with Internet access. This document describes the terms of that access. In addition, a school may decide to create a written agreement or "compact" with parents that expands the terms and responsibilities of the student, parent and school in further detail. However, that written agreement may not permit any Internet or e-mail activity prohibited by this Internet and Device Acceptable Use Policy, and it may not prohibit any such activity permitted by this Policy.

5) Limitations on Internet Usage

A) Personal Safety Violations For Students

SPS strongly recommends that all students follow the two guidelines below, at all times: i) students do not post or transmit photographs or personal contact information about themselves or other people.

ii) Students do not agree to meet with someone they have met online.

SPS does require that student users promptly disclose to their mentor or other school employee any electronic message they receive that is inappropriate or makes them feel uncomfortable.

B) Illegal Activities

All students should be aware that engaging in any of the following illegal activities will result in disciplinary action by their school.

1) Users shall not attempt to gain unauthorized access to the SPS system or to any other computer system through the SPS system, or go beyond their authorized access. This prohibition includes intentionally seeking information about passwords belonging to other users, modifying passwords belonging to other users, illegally obtaining wireless passkeys, or attempting to login through another person's account. Further, users may not attempt to access, copy, or modify another user's files. These actions are not permitted and may be illegal, even if only for the purposes of "browsing."

2) Users shall not attempt to subvert network security, impair the functionality of the network or bypass restrictions set by network administrators. Users are also prohibited from destroying data by spreading computer viruses or vandalizing data, software or equipment.

3) Users shall not use the SPS system to engage in any other illegal act, such as arranging for a drug sale, engaging in criminal gang activity, threatening the safety of a person, etc.

4) Users shall not use the SPS system to download illegal music, books, video, and software without

payment to the originator.

5) Users shall not use software applications that have a continuous connection to the internet that is streaming steadily and consuming large amount of internet bandwidth (e.g. bit-torrent, etc) for the purpose of obtaining illegal content.

C) System Security

1) SPS has adopted the [CIS Critical Security Controls v7](#), security framework to secure and protect student data.

<ol style="list-style-type: none">1. Inventory and Control of Hardware Assets2. Inventory and Control of Software Assets3. Continuous Vulnerability Management4. Controlled Use of Administrative Privileges5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops/Desktops, and Servers6. Maintenance, Monitoring, and Analysis of Audit Logs	Basic Controls
<ol style="list-style-type: none">7. Email and Web Browser Protections8. Malware Defenses9. Limitations and Control of Network Ports, Protocols, and Services10. Data Recovery Capabilities11. Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches12. Boundary Defense13. Data Protection14. Controlled Access Based on the Need to Know15. Wireless Access Control16. Account Monitoring and Control	Foundational Controls
<ol style="list-style-type: none">17. Implement a Security Awareness and Training Program18. Application Software Security19. Incident Réponse and Management20. Penetration Test and Red Team Exercises	Organizational Controls

2) Users are responsible for the use of their individual account if applicable and should take all reasonable precautions to prevent others from being able to use their account. Under no conditions should a user provide their password to another person, except for teachers who may require students to provide their passwords.

3) Student users will immediately notify a teacher if they identify a possible security problem (such as disclosure of their password to another person) and other users will immediately notify the technology team. Users should not attempt to uncover security problems because this may be construed as an illegal attempt to gain access.

4) SPS will install and maintain anti-virus software on each computer and or protection on the network as required. Updates, typically referred to as "virus definitions," will be updated as the manufacturer recommends.

D) Inappropriate Language

All students should be aware that using inappropriate language electronically can be damaging to others and may lead to disciplinary action.

- 1) Restrictions against inappropriate language apply to public messages, private messages, and material posted on Web pages.
- 2) Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, abusive or disrespectful language.
- 3) Users will not post information that could interfere with the educational process or cause a danger of disruption in the educational environment.
- 4) Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
- 5) Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending them messages, they must stop.
- 6) Users will not knowingly or recklessly post false or defamatory information about a person or organization.
- 7) Users should not repost a message that was sent to them privately without permission of the person who sent them the message.
- 8) Users should not post private information about another person.

E) Respecting Resource Limits

- 1) Users will use the system for educational and professional activities.
- 2) Users will refrain from downloading large files unless absolutely necessary. If necessary, users will download the file at a time when the system is not being heavily used.
- 3) Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unsolicited message to many people, except that an unsolicited message sent by a supervisor, relating to work activity does not constitute spamming.
- 4) Users will check their e-mail frequently and delete unwanted messages.
- 5) Users will not send e-mail containing commercial links unless the link is predominantly instructional in nature.
- 6) Users will not use the system to engage in harming or bullying.
- 7) Users should not expect assistance with exporting or importing their email for transference or archival.

F) Plagiarism and Copyright Infringement

- 1) Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
- 2) Users will respect the rights of copyright owners and not infringe on those rights. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the

expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

G) Access to Inappropriate Material

1) Users will not use the SPS system to access material that is profane or obscene (e.g., pornography), that advocates illegal or dangerous acts, or that advocates violence or discrimination towards other people (e.g., hate literature). For students, a special exception may be made if the purpose is to conduct research and is approved by the teacher.

2) If users inadvertently access such information, they should immediately disclose the inadvertent access in a manner specified by their school. This will protect users against an allegation that they have intentionally violated the Internet and Device Acceptable Use Policy.

H) Other

1) Users will not use the Internet for advertising, promotion, commercial purposes or similar objectives.

2) Users will not use the Internet to conduct for-profit business activities or to engage in religious activities. Users are also prohibited from engaging in any non-governmental-related fund raising or public relations activities such as solicitation for religious purposes, lobbying for political purposes, or soliciting votes. SPS is not responsible for this or any other commercial activity users engage in.

3) Users will not rebroadcast or piggyback on existing systems to create personal micro wifi hotspots at any of the schools.

G) E-mail Policy

Email resources are available to all Summit users. Every individual assigned a Summit email address will have the responsibility to use this resource in an efficient, effective, ethical and lawful manner.

A) Email Acceptable Use Guidelines

“Acceptable” e-mail activities are those that conform to the purpose, goals, and mission of SPS and to each user’s responsibilities. Users shall have no right to privacy while using SPS internet or e-mail system. The following actions are prohibited:

1. Opening unknown e-mail attachments or introducing computer worms or viruses. Users are prohibited from performing any activity that will or may cause the loss or corruption of data or the abnormal use of computing resources (degradation of system/network performance).

2. Using e-mail services for private commercial or business transactions and any activity meant to foster personal gain.

3. Conducting non-SPS fund raising or public relations activities such as solicitation for religious and political causes or not-for-profit activities.

4. Transmitting threatening, offensive harassing information (messages or images) containing defamatory, abusive, obscene, pornographic, sexually oriented, racially offensive, or otherwise biased, discriminatory, or illegal material.

5. Attempting to subvert network security, impair functionality of the network, or bypass restrictions set by the network administrators. Assisting others in violating these rules by sharing information or passwords.

6. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations.

B) Account Termination

1. Upon withdrawing from school, all student accounts will be deactivated, and data retained by SPS.
2. Alumni (graduates) of Summit Public Schools will retain access to their SPS email account.

REMINDER: SPS reserves the right to examine any/all e-mail or Internet correspondence for security and/or network management purposes. Violation of this e-mail policy may result in disciplinary action.

H) Device Use

The device resources of SPS are available to authorized students and parents for educational, research, and administrative purposes. In order to maintain this policy, it is essential that the users themselves observe reasonable standards of behavior regarding the use of the devices. The following actions are prohibited:

- Any attempt to modify or damage device, network, or software
- Any attempt to modify the original system configurations
- Improper use of the device equipment
- Installation or use of non-academic games on SPS systems
- Recreational game playing
- Unauthorized use of an SPS account belonging to another user
- Unauthorized reading, use of, or deletion of private files or email belonging to another user
- Sharing username and passwords with other users or any other person
- Any attempt to circumvent (hacking/bypass) system protection and security features
- Knowingly using any system to produce system failure or degrade performance
- Engaging in unauthorized duplication, alteration or destruction of data, programs or software
- Transmitting or disclosing data, programs or software belonging to others or duplicating copyrighted materials
- Use of device resources for private purposes, including, but not limited to, the use of device resources for profit making or illegal purposes

SPS reserves the right to investigate any of the above abuses, as well as any other interference with the proper functioning of the SPS network or infringements upon another user's rights. Any violation will result in disciplinary action. Consequences vary from school site to school site which may include suggested payments for damages and or restorative practices if payment is limited or not possible. The school's Executive and/or Assistant Director will make the final decision.

a) Take Home Policy:

This Internet and Device Acceptable Use Policy continues to be applied to all students. The technology resources provided are intended for student learning, therefore the policies must be adhered to for both safety and compliance.

b) Chromebook Care Manual:

All students must adhere to the [care manual](#) to ensure their device is working properly. This guide has been provided to address in-school and out-of-school use. The guide is not comprehensive, rather it

focuses on the most common guidelines and practices for taking care of student devices. An electronic version will be provided to all families during the start of the new academic year.

c) Mini-Sheet Device Care Manual:

All students will not alter or damage or discard the [guide](#). The mini-guide is in reference to the Chromebook Care Manual and highlights the most important “to do” to ensure your device is properly working.

I) Bring Your Own Device (BYOD)

SPS does not formerly recognize or endorse student BYOD preferences, but understand the device preferences of each student. SPS strives to ensure every single student has a dedicated device to enable their academic success, hence are preferred and in our opinion best tool for student learning is the Google Chromebook. Our recommendation is based on our learning model, applicable standardized tests, and ease of intuitiveness for all learners.

a) Wireless Network Access:

Although we strive to provide maximum capability to all devices, due to our robust information security policies, we recommend only the most recent devices will most likely be compatible with our network and security standards. (Ideally, any device that is older than 4 years may have have challenges connecting to our network).

b) Online Content Filter:

Summit deploys content filtering to ensure compliance with the Children’s Internet Protection Act (CIPA). All internet content will be filtered as well as additional safeguards are implemented to limit excessively large bandwidth consumption activities.

c) Intrusion Detection and Prevention:

SPS has also implemented sophisticated IDP to address cyber external and internal malicious activities to ensure the network and its students are protected from attacks.

J) Cyberbullying

Bullying through the use of technology or any electronic communication (including, but not limited to, a transfer of signs, signals, writing, images, sounds, data or intelligence of any nature) transmitted by the use of any electronic device (including, but not limited to, a computer, telephone, cellular telephone, text messaging device or personal digital assistant) is prohibited. California anti-bullying laws is enforced by the following: California Education Code 32261-32262, 32265, 32270, 35294.2, and 48900. Washington anti-bullying laws is enforced by the following Washington State Legislature RCW 9A.36.080(3), 28A.300.285, 28A.300.2851, 28A.600.480, 43.06B.060, 392-190-057, 293-190-058

These actions are prohibited:

- Flaming
- Denigration also known as "dissing"
- Bash boards
- Impersonation
- Outing
- Trickery
- Exclusion

- Harassment
- Happy slapping
- Text wars or attacks
- Negative Online polls
- Sending malicious codes
- Griefing

Users should always use good digital citizenship when posting or replying on the internet. Always be kind, have common courtesy, and be considerate to others. Displaying online social behaviors that model good cyber citizenship is important and encouraged.

K) Cyber Incidents

SPS believes in ensuring all students and faculty are safe online. All incidents reported will be thoroughly investigated by the Chief Technology Officer and members of the Information Security Committee and the Information Security Governance Team. The outcomes and additional actions will be handled by the Executive and its designated administrators at their respective schools.

a. Reporting an incident:

Report all concerns or incidents directly to school leaders.

b. Follow-up and Actions:

School leaders will coordinate and provide follow-up on all incidents or concerns reported.

K) Google Workspace for Education Notice & Consent ADDENDUM

Effective Date: 10/1/2025

Applies to: All Summit Public Schools faculty, staff, students, and parents/guardians

1. Account Provisioning

Summit Public Schools (SPS) provides students with a Google Workspace for Education account to facilitate learning, collaboration, and communication. This account is a "Core Service" managed by the district and includes tools such as Gmail, Google Drive, Calendar, and Classroom.

2. Information Collected by Google

To provide these services, Google may collect and use certain information, including:

- **Personal Information:** Name, email address, and password provided by SPS to create the account.
- **Usage Information:** Device information, log information (IP address, date/time of access), and location information related to the use of the services.
- **Content:** Any information or files created, saved, or shared by the student within the Google Workspace environment.

3. Core vs. Additional Services

- **Core Services:** Google does not use personal information from "Core Services" for advertising

purposes or to create advertising profiles.

- **Additional Services:** Students may access "Additional Services" such as YouTube or Google Maps for educational research. These services may collect and use personal information differently than Core Services. By signing this policy, parents/guardians provide explicit consent for students to access these Additional Services for school-related purposes.

4. Parental Rights and Control

Parents have the right to:

- **Review Data:** Request to see the personal information SPS has shared with Google.
- **Limit Access:** Request that SPS disable a student's access to specific "Additional Services".
- **Delete Accounts:** Request the deletion of a student's account at any time, noting that this may impact the student's ability to participate in certain digital learning activities.

5. Legal Compliance

This notice and the associated parental signature ensure compliance with the **Family Educational Rights and Privacy Act (FERPA)**, the **Children's Online Privacy Protection Act (COPPA)**, and applicable state laws in California and Washington.\

https://workspace.google.com/terms/education_terms/

L) ARTIFICIAL INTELLIGENCE (AI) TOOLS ADDENDUM

Effective Date: 10/1/2025

Applies to: All Summit Public Schools faculty, staff, students, and parents/guardians

A. PURPOSE

Summit Public Schools ("SPS") recognizes that Artificial Intelligence (AI) technologies can enhance teaching, learning, and operational efficiency. This addendum outlines how AI tools may be used responsibly within Summit's educational and administrative environments, in alignment with existing Internet and Device Acceptable Use Policies.

B. DEFINITIONS

- **Artificial Intelligence (AI):** Software or systems capable of generating text, images, code, or other content, or making predictions, recommendations, or decisions using machine learning or similar techniques.
- **Approved AI Tool:** Any AI system or platform reviewed and approved by the SPS Technology Department for educational or administrative use.
- **Personally Identifiable Information (PII):** Any data that could identify a student or staff member, including but not limited to names, addresses, grades, or unique identifiers.

C. STUDENT USE OF AI

1. Authorized Educational Use: Students may use district-approved AI tools only for instructional purposes as directed by teachers or administrators.
2. Prohibited Use:
 - a. Entering personally identifiable information into any AI tool not explicitly approved by SPS.
 - b. Submitting AI-generated work as original without attribution or approval.
 - c. Using AI to bypass academic expectations, plagiarize, harass, or produce inappropriate content.
3. Academic Integrity: Students must acknowledge when AI tools are used to assist in academic work and comply with school-specific integrity guidelines.
4. Digital Citizenship: Students are expected to apply critical thinking, verify accuracy, and uphold respect and responsibility in all AI interactions.

D. FACULTY AND STAFF USE OF AI

1. Professional Conduct: Faculty and staff may use AI tools to enhance instruction, communication, or administrative efficiency. However, they must:
 - a. Verify the accuracy, bias, and appropriateness of all AI-generated content.
 - b. Ensure human oversight in all grading, evaluation, or decision-making processes.
 - c. Avoid uploading or sharing confidential, student-identifiable, or proprietary data with AI systems unless explicitly authorized by the CTO.
2. Training and Support: SPS will provide professional learning opportunities to promote AI literacy and responsible classroom integration.

E. DATA PRIVACY AND SECURITY

- Legal Compliance:
 - All AI use must comply with:
 - FERPA (Family Educational Rights and Privacy Act)
 - COPPA (Children's Online Privacy Protection Act)
 - CIPA (Children's Internet Protection Act)
 - Applicable state student data privacy laws (CA Ed. Code §49073.1; WA RCW 28A.604).
- Data Handling:
 - AI tools may not store, analyze, or transmit identifiable student data beyond the educational purpose authorized by SPS.
 - Vendors must sign a Data Privacy Agreement (DPA) before use in classrooms or district operations.
- Monitoring and Oversight:
 - The SPS Technology Department reserves the right to monitor AI tool use to ensure compliance, data security, and educational appropriateness.

F. TRANSPARENCY AND PARENT/GUARDIAN NOTICE

- Parents and guardians will be notified annually if SPS-authorized AI tools are used for instruction.
- By signing the Student/Parent Acceptable Use Policy, parents acknowledge and consent to the use of approved AI tools in accordance with this addendum.
- Parents may request more information about approved AI tools or opt-out of optional AI-enhanced learning experiences.

G. ENFORCEMENT

- Violations of this AI Addendum will be treated as violations of the Summit Public Schools Internet and Device Acceptable Use Policies.
- Disciplinary actions will follow the established graduated discipline process for students and the employee discipline process for faculty and staff.

H. POLICY REVIEW

This addendum will be reviewed annually by Summit Public Schools to ensure ongoing compliance with emerging laws and best practices in AI ethics, data protection, and education.

By signing this page, I hereby agree that I have read and understood the “Summit Public Schools: Internet and Device Acceptable Use policy” and agree to adhere to its terms and conditions.

Student Name _____ Date _____

Student Signature _____

Parent Signature _____