The Preston School District No. 201 provides its students and staff access to a multitude of technology resources to enhance learning, as the board recognizes the importance of providing positive, productive educational experiences through the district's Internet, computer, and network services (hereinafter, "technology resources"). However, the privilege of access to the district's technology resources also comes with the responsibility of students, teachers, staff and the public to exercise appropriate use of these resources. District policies are intended to promote the most effective, safe, productive, and instructionally sound uses of technology resources. District technology resources are to be used primarily for professional and/or educational purposes and are not a public forum for general use.

EXPECTATIONS AND PROHIBITIONS

The district uses its information and technology resources in safe, legal, and responsible ways. Responsible use of the district's technology resources is expected to be ethical, respectful, academically honest, and supportive of the district's mission. Each computer user has the responsibility to respect every other person in our community and on the Internet. Digital storage and electronic devices used for school purposes will be treated as extensions of the physical school space. Administrators or their designees may review files and communications (including electronic mail and social media) to ensure that users are using the district's technology resources in accordance with district policies. Users should not expect that files stored on servers, discs, or the cloud will be private. Users should also understand that school servers regularly record Internet activity in log files.

Users are expected to abide by the law and generally accepted rules of network etiquette. The following guidelines and prohibitions are intended to clarify expectations for conduct, but they should not be construed as all-inclusive.

1. Transmission of any material in violation of any local, state, or federal law is strictly prohibited. This includes, but is not limited to sending, receiving, viewing or downloading materials that are: deemed to be harmful to minors, as defined by Idaho Code §18-1514; copyrighted; streamed; licensed or proprietary; information that includes any personally identifiable information about students or employees; defamatory or discriminatory; threats; or threatening or obscene. This also includes any activity that involves the sale, purchase, or promotion of illegal items or substances.
2. Intentional or unintentional use of technology resources to access or process proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.
3. Software and/or services may only be installed or downloaded on school devices if they are consistent with educational use and approved by the district.
4. Use of district technology resources for commercial activities, product advertisement, religious activities, or political lobbying is prohibited.
5. It is a violation of this policy to use district technology resources to gain unauthorized access to district networks, servers and other technology resources or to other network systems through hacking or other illegal activities. Users may be held personally and

financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware, and/or unauthorized costs incurred. All users are required to use reasonable care to protect passwords and to otherwise ensure that district technology resources are not used to breach system security.

6. Files stored on district-managed networks are the property of the district and, as such, may be inspected at any time and should not be considered private.
7. Materials published for electronic publication must be for educational purposes. School administrators, teachers, and staff may monitor these materials to ensure compliance with content standards.
8. Use of electronic devices in school, regardless of ownership, should be consistent with the district's educational objectives, mission and curriculum.
9. Students may use district-provided equipment (e.g., laptops, tablets, or Chromebooks) only in accordance with Policy 694 – District-Provided Mobile Computing Devices. Students may use cell phones and other personal communication devices only in accordance with Policy 518 – Student Use of Personal Communication Devices. Improper use or care of district-provided equipment or technology resources is a violation of district policy and may be grounds for discipline as provided by district policy. Improper use or care of district-provided technology includes, but is not limited to: engaging in spamming; attempting to damage district technology, files, or data; alteration of configured equipment, including the addition of unauthorized passwords and user accounts; installing, uploading or downloading unauthorized programs; copying district software for personal use; or using district technology for personal business, unapproved fundraising, or personal advertising.
10. Users will not use district technology resources, including electronic mail, to engage in bullying or cyberbullying in violation of the district's bullying and harassment policies. This prohibition includes using any technology or other electronic communication off school premises to the extent that student learning or the school environment is substantially and materially disrupted.
11. The district respects the right of employees and students to responsibly use social media and networking sites, message boards and forums, as well as personal websites and blogs. Personal use of these sites should not damage the reputation of the district, its employees, students, or their families, and should be consistent with the district's educational objectives, mission, and curriculum.

ACCESS TO DISTRICT TECHNOLOGY

Access to district technology resources will be provided to employees and students in an expedient manner following employment by or enrollment in the district and signature of the Acceptable Use Agreement (see Policy 942F1). The agreement outlines district expectations regarding technology use. This agreement may be modified by the district as necessary at any time. The district will make the final determination as to what constitutes unacceptable use and its decision is final. The agreement is provided so that users are aware of the responsibilities they acquire. No individual shall access district technology resources without all required agreement signatures.

INFORMATION CONTENT AND USES OF THE SYSTEM

Commercial uses of district technology by staff or students are strictly prohibited. Users shall not sell or offer for sale any goods or services that could be construed as a commercial enterprise. The district may choose to provide means for staff to offer goods for sale on a non-enterprise basis. Any form of gambling is prohibited. The technology is to be used primarily for professional and/or educational benefit.

PRIVACY

Use of the district's technology resources is a privilege and not a right. Access has not been established as a public access service or a public forum. The district reserves the right to monitor, inspect, copy, review, delete, and/or store at any time and without prior notice any and all results of usage of the Internet, computers, network resources, and any and all information transmitted or received in connection with such usage. This includes the right at any time to investigate and review the contents of employee e-mail files and other files created or saved to the district's network or computers. School district employees should be aware that data and other materials in files created, stored, sent, received, displayed, or maintained in district computers, including personal files, may be subject to review, disclosure or discovery under the Idaho Public Records Act (Idaho Code §§74-101 *et seq*.). All such information will be and remains the property of the district and users have no expectation of privacy regarding such materials. The district has the right to place restrictions on the use of the district's Internet, computers, and network resources and may also deny access to staff and students who violate related policies and procedures.

Posting of Personally Identifiable Information

Users of district technology resources will not use the system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including but not limited to, address, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs, or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without the permission of the person who sent the message.

The limitation on posting of personally identifiable information set forth in this policy does not prohibit the posting of employee contact information on school websites or communication between employees and other individuals when such communications are made for education-related purposes (i.e., communications with parents or other staff members related to students).

Employees creating or posting school-related webpages may include personal contact information about themselves on a webpage. However, employees may not post contact information about students unless:

1. Such information is classified by the district as directory information as defined by the district in accordance with the Family Educational Rights and Privacy Act ("FERPA") and verification is made that the district has not received notice from a parent/guardian or eligible student that such information is not to be designated as directory information; or
2. Such information is not classified by the district as directory information but written consent for release of the information to be posted has been obtained from a parent/guardian or eligible student.

In addition, prior to posting any personal contact or personally identifiable information on a school-related webpage, employees shall obtain written approval of the content of the postings in accordance with applicable district policies and procedures.

The prohibitions set forth herein specifically prohibit a user from utilizing the district's technology resources to post personal information about a user or another individual on social networks including but not limited to, Facebook, Snapchat, Twitter (X), TikTok, Instagram, Reddit, and similar websites or applications.

EMPLOYEE RESPONSIBILITIES

Employees are responsible for safeguarding the district's equipment while in the employee's possession and/or responsibility. Employees shall immediately (within 24 hours) report to his/her supervisor if the equipment is lost or stolen. Employees are prohibited from allowing any third party to use district-owned or leased equipment.

Employees must use district technology in a professional, legal, and responsible manner. Use of district technology for personal business must be kept to a minimum and must conform to district policies and procedures and state and federal laws and regulations. In accordance with Idaho law, employees are prohibited from downloading or using the TikTok application or visiting the TikTok website on any network owned, operated, or otherwise used by the district, including district-issued cell phones, computers and other devices capable of Internet connectivity.

When acting within the capacity of a district employee, communication from any location and using any type of equipment, owned by the district or otherwise, must reflect professional integrity and responsibility and not have an adverse effect on students or on the performance of an employee's duties for the district. Employees are required to immediately report any violations of this policy to their principal or immediate supervisor.

All district-owned or leased equipment provided to employees shall be immediately returned to the employee's supervisor upon request or upon termination of the employee's employment relationship with the district.

Employee Email

All employees are assigned a district email account, which should be used for all official business. Employees must use their district email account when acting in the capacity of a

school district employee and when corresponding with parents or students. Employees may not use their district-assigned email address for communications on social media networks without prior district approval.

Employee Communications with Students

The board recognizes that there are occasions when school district employees may have a legitimate educational need to communicate with a student outside of school hours. Any communication between a district employee and a student via telecommunications, text messages, e-mails, and/or any other medium must have an educational purpose and be professional in content and tone. Employees who engage in such communications with students are expected to act as representatives of the district. Employees, including coaches, should include an administrator or another adult in messages to students. Any communications with students may be subject to review by the district. Employees will not make any statements or forward information that could reasonably be believed to violate this policy, other district policies, or state or federal law. At the discretion of the superintendent or designee, employees may be required to copy all such communications to students to the building administrator or designee.

If an employee receives any communication from a student that is inappropriate or creates concerns, the employee is obligated to report such communication to the building administrator or designee.

INTERNET SAFETY FOR STUDENTS

With respect to any of its computers with wireless Internet access, the district will utilize filtering software or other technologies to (1) prohibit and prevent the use of school computers and other district owned technology-related services from sending, receiving, viewing, or downloading materials that are obscene, contain child pornography, or are deemed harmful to minors as defined in Idaho Code §18-1514 or 47 U.S.C. §254(h); or (2) filter or block internet access to obscene materials, materials harmful to minors, and materials that depict the sexual exploitation of a minor as defined in Idaho Code §18-1507. The district will also monitor the online activities of students through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material that is inappropriate for minors.

The district's filtering solution will include the ability:

1. For the district to manage its own filtering policies, including the decision to block specific categories of content and to maintain its own whitelist and blacklist overrides;
2. To provide the district utilization and filtering reports, including the most frequently visited websites, the most frequently visited categories, the most frequently blocked websites, the most frequently used search terms, and the top authenticated users;
3. To audit all changes to content filtering; and
4. For all reporting and management of content filtering to be available through any internet-connected browser and efficiently perform all content filtering functions.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other education projects being conducted by students age 17 and older.

The district's instructional program will include a component on Internet safety for students and appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms or on instant messaging platforms, and cyberbullying awareness and response.

In accordance with Idaho Code §33-132, the district will require that every vendor, person, or entity providing digital or online library resources to the district for use by students to verify that they have safety policies and technology protection measures that:

1. Prohibit and prevent a user from sending, receiving, viewing, or downloading materials that are deemed to be harmful to minors as defined in Idaho Code §18-1514; and
2. Filter or block access to obscene materials, materials harmful to minors, and materials that depict the sexual exploitation of minors as defined in chapter 15, title 18, Idaho Code.

Notwithstanding any contract provision to the contrary, the district may withhold further payments, if any, to any provider of digital or online library resources if the provider fails to comply with the requirements of this policy.

CREATION AND USE OF DISTRICT SOCIAL MEDIA SITES

District social media sites exist for school district employees to promote events, student success stories, clubs, athletics, and other programs related to the education of students. Employees may create social media sites in accordance with this policy and procedures approved by the superintendent or designee. All district social media sites should be used to support the district's educational mission.

Once a social media site is approved in accordance with applicable procedures, it is the responsibility of all users to carefully consider their behavior and what they place online when communicating with or "friending" any individual. Users are responsible for complying with all district policies and procedures related to use of school district technology resources and applicable state and federal laws. Users may not disrupt the learning environment, educational programs, school activities or the rights of others. District administration is authorized to access and monitor all school district social media sites and postings made to district social media sites using district servers, computers, networks, and related technology under the direction of the superintendent or designees, law enforcement, or a court order, subpoena, or other legal action or authority.

The district's authority to inspect, review, or retain electronic communication created, sent, displayed or received using the district's technology resources applies no matter where the use

occurs, whether brought onto school district property, at district events, connected to a district network, or when using mobile computing equipment and telecommunications facilitated in protected and unprotected areas or environments directly from home or indirectly through another social media or Internet service provider, as well as by other means. All actions must be conducted in accordance with local, state, and federal law, assist in the protection of district resources, insure compliance with district policies and procedures, and social media and Internet service provider terms and conditions.

CONSEQUENCES FOR INAPPROPRIATE USE

All users must fully comply with this policy and the Acceptable Use Agreement and are expected to immediately report any violations or suspicious activities to the building principal or designee. Any action that violates district policy or procedures or is determined by an administrator to constitute an inappropriate use of district technology resources or social media sites or otherwise violates the Acceptable Use Agreement is strictly prohibited. Failure to comply with this policy or the Acceptable Use Agreement may result in usage restrictions, loss of access privileges, and/or disciplinary action up to and including termination of employment, recommendation for student expulsion, and/or other legal action. The superintendent or designee may also report the violation to law enforcement where appropriate.

Users are responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

WARRANTIES, LIMITATION OF LIABILITY AND INDEMNIFICATION

The district makes no warranties of any kind, express or implied, with respect to its provision of access to and use of its computer networks and the Internet provided under this policy. Use of the district's system is at the user's own risk and is provided on an "as is, as available" basis. The district will not be responsible for any damages users may suffer, including but not limited to, loss, damage, or unavailability of data stored on district diskettes, tapes, hard drives, or servers, or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause.

The district is not responsible for the accuracy or quality of any advice or information obtained through or stored on the district's system. The district will not be responsible for financial obligations arising through unauthorized use of the district's system or 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 networks or the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user and attorney fees.

The user or, if the user is a minor, the user's parents/guardians, agree to cooperate with the district in the event the district initiates an investigation of a user's use of their access to its computer network and the Internet.

IMPLEMENTATION, NOTICE AND POLICY REVIEW

The superintendent or designee may develop appropriate forms, guidelines, and procedures necessary to implement this policy. The district will inform staff, students, parents/guardians and other users about this policy through posting on the district website and by other appropriate methods. A copy of this policy will be available for review at the district office. The district will also file this policy with the state superintendent of public instruction every five (5) years after initial submission and subsequent to any amendments to this policy thereafter. By accessing the district's Internet, computers and network resources, users acknowledge awareness of the provisions of this policy and awareness that the district uses monitoring systems to monitor and detect inappropriate use.

♦ ♦ ♦ ♦ ♦ ♦ ♦

LEGAL REFERENCE:

Idaho Code Sections
- 18-1507 – Definitions – Sexual Exploitation of a Child – Penalties
- 18-1514(6) – Obscene Materials – Definition (Harmful to Minors)
- 18-2201 – Computer Crime – Definitions
- 18-2202 – Computer Crime
- 18-6726 – TikTok Use by State Employees on a State-Issued Device Prohibited
- 33-132 – Local School Boards – Internet Filtering Required
- 33-506(1) – Organization and Government of Board of Trustees
- 33-512 – Governance of Schools
- 74-101 *et seq*. – Idaho Public Records Act

U.S. Code Sections
- 20 U.S.C. §9134(f) – State Plans – Internet Safety (Libraries)
- 20 U.S.C. §7131 – Internet Safety
- 47 U.S.C. §254(h) – Universal Service (Telecommunications Services for Certain Providers)

CROSS-REFERENCE:

442 – Code of Ethics for Certificated Employees
518 – Electronic Communication Devices

694 – District-Provided Mobile Computing Devices
962 – Use of District Trademarks, Service Marks and Social Media

ADOPTED: July 16, 2025

AMENDED:

**Language in text set forth in italics is optional.*