Lake Stevens School District
POLICY 1800F-2
Adopted: 8-12-26
Revised: 9-16-26

LSSD Staff Acceptable Use Agreement (AUA)

To be signed by all staff during the onboarding process.

SCOPE AND NETWORK USE

By signing this agreement, staff confirm they have read and understand the Lake Stevens School District Electronic Resource Policy and Procedures 1800, as well as the district Privacy Policy. These procedures apply to all district staff and cover all aspects of the district network, which includes wired and wireless computers/devices and peripheral equipment, files and storage, e-mail, Internet content, and all computer software, applications, or resources licensed to the District.

The District expects staff to exercise good judgment and use the computer equipment in an appropriate and professional manner. Use of the equipment is expected to be related to the District's goals of educating students and/or conducting District business. Incidental and occasional personal use that is infrequent or brief in duration is permitted so long as it occurs on personal time, does not interfere with District business, and is not otherwise prohibited by District policy or procedures.

Staff members who supervise students, assign digital devices, or observe student technology use are required to make a reasonable effort to monitor that use. Active supervision ensures that student online activity remains safe and aligns with the educational mission of the district. Furthermore, staff are expected to maintain a working familiarity with the digital tools and platforms used in their classrooms so they can effectively instruct, assist, and guide students in safe, appropriate online behavior and digital citizenship.

DOCUMENT MANAGEMENT, DATA PRIVACY, AI AND SOFTWARE

The District prioritizes the security, confidentiality, and legal compliance of all district records and student data. To ensure proper data governance, staff must adhere to the following procedures regarding document management, privacy, and software usage:

- Document Storage and Public Records: All documents related to the conduct of District business and all educational records identified in Policy 5230 Student Records shall be stored on District-provided systems and storage services. Using any cloud or personally-acquired document management or storage service for district business is prohibited. Additionally, all documents, files, and electronic communications are subject to the public records disclosure laws of the State of Washington, including Washington's Public

Records Act RCW 42.56.

- Student Data and Privacy: District staff must maintain the confidentiality of student data and adhere to all applicable federal and state privacy laws. This includes the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), and Washington state student privacy laws (including the SUPER Act, RCW 28A.604, and RCW 28A.605.030). To ensure compliance, staff must only use district-approved and vetted digital tools or services when handling student information. Additionally, publishing any student work or identifying media online requires explicit permission from the parent or guardian.

- Ethical Use of Artificial Intelligence**:** Regarding artificial intelligence, staff must never input personally identifiable information (PII), confidential student data, or sensitive district information into unauthorized, unvetted, or public generative AI tools. Furthermore, staff should employ a "Human-AI-Human" framework when using these tools; this means starting with human intent, using AI for generation or brainstorming, and applying human review to the final product. Staff must ensure transparent use of AI-generated content in their workflows and diligently check all AI outputs for potential bias, hallucinations, or inaccuracies before utilizing them in a professional or educational capacity.

- Software Permissions and Account Lifecycle: Users must receive permission from the District prior to loading non-District software onto District equipment, and all software must be legally licensed prior to loading. Finally, all district-provided network and workspace accounts (along with associated files) will be deactivated and deleted upon a staff member's resignation or termination.

- Ownership of Work: All digital content, files, and work products created by employees as part of their employment—including any derivative works—are considered the property of Lake Stevens School District, unless a formal written agreement states otherwise. Staff members must obtain explicit permission from a student (and their parent/guardian, when appropriate) prior to sharing, publishing, or distributing the student's original work to parties outside of the school.

- Educational Applications and Programs: Prior to requesting students to download or sign up for educational applications or programs, staff will review “terms of use,” “terms of service,” and/or “privacy policy” of each application or program to ensure that it will not compromise students’ personally identifiable information, safety, and privacy. Staff should also, as appropriate, provide notice to students’ parents/guardians that the staff person has requested that students download or sign up for an application or program.

- Accessibility of Electronic Resources: Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the district. To ensure that individuals with disabilities have equal access to district programs, activities, and services, the content and functionality of websites associated with the district should be accessible. Such websites may include, but are not limited to, the district’s homepage, teacher websites, district-operated social media pages, and online class lectures. District staff with authority to create or modify website content

or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities.

UNACCEPTABLE/PROHIBITED USE

Unacceptable network use by staff includes, but is not limited to:

- Commercial Use: Using the network for personal or private gain, personal business, or commercial advantage.
- Political Use: Assisting or advocating, directly or indirectly, for or against a ballot proposition and/or the election of any person to any office.
- Illegal or Indecent Use: Using the network for illegal, bullying, harassing, vandalizing, inappropriate, or indecent purposes (including accessing, storing, or viewing pornographic, indecent, or otherwise inappropriate material).
- Disruptive Use: Interfering or disrupting other users, services, or equipment, such as distributing "Spam", propagating viruses, or unauthorized access/destruction of District computers.
- Personal Entertainment Use: Storing personal entertainment/media files on the network.
- Wearable Technology: To protect student and staff privacy, ensure safe learning environments, and maintain professional boundaries, strict guidelines apply to "smart glasses and AI-enabled wearable devices" (any body-worn device capable of capturing media, transmitting data, or using AI to analyze surroundings).
    - General Restrictions: Recording audio, video, or taking photos of students or staff using personal wearable devices is strictly prohibited. Additionally, these devices (e.g., smartwatches, smart glasses) must not be used to bypass the district's internet filter.
    - Perception of Impropriety: Wearing and using discreet wearable recording technology creates a "perception of impropriety." While there are legitimate times to film students (e.g., class assignments, sports competitions, or district social media), staff must maintain appropriate professional boundaries by using a traditional camera or cell phone where the act and purpose of filming are obvious.
    - Prohibited Times and Contexts: Staff may not wear or use AI or camera-enabled devices (e.g., smart glasses) at any time students are present—including instructional time, coaching, and supervision duties such as assemblies or fire drills. Furthermore, to respect workplace civility and privacy, these devices may not be used to film colleagues.
    - Prohibited Areas (Non-Negotiable): Use or possession (active or inactive) is strictly prohibited in bathrooms, locker rooms, health/counseling spaces, special education meetings (IEP/504), and any setting involving confidential student information.
    - Exceptions and Accommodations: Any exceptions or accommodations requiring the use of wearable technology to record audio and/or video of students or staff must be explicitly approved in advance by both the building administration.
    - Future-Proofing: This policy applies to all current and future wearable technologies with similar capabilities, regardless of brand or form.
- Unauthorized Devices/Hotspots: Using personal wireless hotspots or connecting unauthorized personal devices to the internal district network is prohibited.
- Professional Boundaries: Staff must maintain professional boundaries in digital spaces, including prohibitions against interacting with students on personal social media accounts or texting them from personal phone numbers.
- Endangering Others: Posting, sending, or storing information online that could endanger others (e.g., bomb construction, drug manufacturing).
- Wasting Resources: Intentionally wasting limited network or technology resources.

PERSONAL DEVICES & GUEST NETWORK (BYOD)

Lake Stevens School District provides a guest network to support educational and professional activities. The use of personal devices (smartphones, laptops, tablets, etc.) on any LSSD network is a privilege, not a right. When connecting a personal device to district Wi-Fi, users must adhere to the following strict guidelines:

- Right to Inspect: Should personal equipment be used on the district's networks, the district reserves the right to gain access to the device for analysis to resolve any identified security issues, network disruptions, or cyber threats. As a condition of using the district's networks, a user must provide the requested device to district administration or IT staff immediately upon request.
- Strict Prohibition of Filter Bypassing: Attempting to defeat, bypass, or disable the district's Internet filter using a personal device is strictly prohibited. This includes, but is not limited to, the use of Virtual Private Networks (VPNs), proxy servers, anonymizers, or dark web browsers (such as the Tor browser).
- Network Integrity: Using personal wireless hotspots or connecting unauthorized personal devices to the internal, secured district network is prohibited. All personal devices must connect only to the designated Guest network.
- Liability: Lake Stevens School District is not responsible for damages, loss, theft, or any cost incurred to personal digital technologies or electronic communication devices while on district property or connected to the district network.

NETWORK SECURITY

Passwords and Multi-Factor Authentication (MFA) are the first lines of defense for a user account. System logins and accounts are to be used only by the authorized owner of the account and for authorized district purposes. Staff are responsible for all activity on their account and must not share their account password or MFA credentials.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy, utilizing a minimum of 15 characters;
- Enroll in and utilize Multi-Factor Authentication (MFA) to access district systems and data;
- Utilize the district's Single Sign-On (SSO) portal whenever possible to access authorized applications securely;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight and secure;
- Do not store passwords in a file without encryption;
- Do not use the remember password feature of Internet browsers; and
- Lock the screen or log-off if leaving the computer.

PRIVACY

The District network, computers, Internet, and use of e-mail are not inherently secure or private. Users are urged to be caretakers of their own privacy and to not store sensitive or personal information on District computers. The District may monitor and review electronic information in order to analyze the use of systems or compliance with policies, conduct audits, review performance or conduct, obtain information, or for other reasons.

The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of the network; user files and disk space utilization; user applications and bandwidth utilization; user document files, folders and electronic communications; e-mail; Internet access; and any and all information transmitted or received in connection with network and e-mail use. Communications may not be encrypted so as to avoid a security review.

The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington. Backup is made of all district e-mail correspondence for purposes of public disclosure, disaster recovery, and records retention. The District is not responsible for any damages suffered by the user, including loss of data due to service interruptions, or for any unauthorized financial obligations resulting from the use of the district's network or the Internet. The district will provide a procedure for students and staff members to anonymously request access to Internet websites blocked by the district's filtering software. The district will also provide an appeal process for requests that are denied.

COPYRIGHT AND DISCIPLINE

Downloading, copying, duplicating, and distributing copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately. Violation of any conditions of use could be cause for disciplinary action, up to and including revocation of network access privileges, restitution, discharge, and/or a police report.