Lake Stevens School District
POLICY 1800F-3
Adopted: 8-12-26

LSSD Student Responsible Use Agreement (RUA)

To be signed by student and parent

STUDENT NETWORK ACCEPTABLE USE

By signing this agreement, the student and parent/guardian confirm they have read, discussed, and agree to Lake Stevens School District Policy 1800, Electronic Resources, and the district Privacy Policy. The district network includes wired and wireless computers/devices, peripheral equipment, files and storage, e-mail, Internet content, and all computer software, applications, or resources licensed to the District. Use of the equipment is expected to be related to educational purposes.

- CIPA & COPPA Compliance: Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Attempts to bypass or disable the filter are prohibited. The district also adheres to the Children's Online Privacy Protection Act (COPPA) regarding online information gathering. By signing this agreement, parents grant permission for the district to create necessary digital educational accounts for their child.
- FERPA Compliance: Student data confidentiality is maintained in accordance with the federal Family Educational Rights and Privacy Act (FERPA) and state laws.
- Prohibited Use & Discipline: Using the District Network for personal or private gain, personal business, or commercial advantage is prohibited. Using District Network for political purposes in violation of federal, state, or local laws is prohibited. Using the District Network for illegal, bullying, harassing, vandalizing, inappropriate, or indecent purposes is prohibited. Additionally, students must not intentionally waste limited network resources or post, send, or store information online that could endanger others (e.g., bomb construction, drug manufacturing). Violation of any conditions of use could be cause for disciplinary action, including suspension or expulsion from school, and suspension or revocation of network and computer access privileges.
- Wearable Technology: Personal wearable devices (e.g., smartwatches, smart glasses) must not be used to bypass the district's Internet filter. Recording audio, video, or taking photos of students or staff using these devices is strictly prohibited. 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 and the Technology Department.
- Unauthorized Devices/Hotspots: Using personal wireless hotspots or connecting unauthorized personal devices to the internal district network is prohibited.
- Digital Citizenship: Communicate only in ways that are kind, responsible, respectful and

lawful. Lake Stevens School District email should only be used for school-related email and projects.

- Internet Safety Instruction: All students will be educated about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.
- Ethical AI Use**:** Students must follow teacher guidelines regarding appropriate use of AI tools for specific assignments. To protect privacy and safety, students must never input personally identifiable information (PII) of themselves or others - such as full names, addresses, passwords, or student ID numbers - into any generative AI tool. When authorized to use AI, students must engage in transparent use by clearly citing or attributing how AI was utilized in their process. Submitting AI-generated content as one's own original work without proper attribution or permission is a violation of academic integrity. Additionally, students are expected to practice a "Human-AI-Human" framework by critically evaluating AI outputs and checking information for bias and inaccuracies before incorporating it into their assignments.
- Account Lifecycle: District-provided digital accounts and associated files will be deactivated and deleted upon a student's graduation, promotion out of the district, or withdrawal.
- Ownership of Work: Students retain ownership of the original digital work they create as part of the regular instructional program. However, if a student creates work while acting as a district employee or under a paid agreement with the district, that work becomes district property.

PERSONAL DEVICES & GUEST NETWORK (BYOD)

Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school. Lake Stevens School District provides a guest network to support educational 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 student 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 are the first level of security 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. Students are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- 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;
- 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.

GENERAL DEVICE CARE

Students must treat all district digital technologies, including cart-based classroom Chromebooks, with care. Any damages must be reported immediately to a teacher or other district staff member. Intentional vandalism or destruction of district property may result in disciplinary action or financial responsibility.