Lake Stevens School District
POLICY 1800P
Adopted: 6-12-96
Revised: 8-8-01
Revised: 2-23-11
Revised: 5-23-12
Revised: 8-12-26
Revised: 9-16-26

PROCEDURES:

These procedures are written to support the Electronic Resources policy of the Board of Directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful technologically fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career. Expectations for student and staff behavior online are no different than face-to-face interactions. To empower our community to achieve these ideals, the core principles of these procedures are embedded within the Acceptable Use Agreement for staff , the Responsible Use Agreement for students , and the Device Loan Agreement.

NETWORK

The district network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, etc.). The District reserves the right to prioritize the use of, and access to, the network. All use of the network must support education and research and be consistent with the mission of the district.

ACCEPTABLE NETWORK USE BY STAFF AND STUDENTS

- Creation of files, projects, videos, web pages, and podcasts using network resources in support of educational research;
- Participation in blogs, wikis, collaborative workspaces, social networking sites, and groups and the creation of content for podcasts, e-mail, and web pages that support educational research;
- With parental permission, the online publication of original educational material, curriculum related materials, and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district policies and guidelines;
- Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the district network after checking with the District's Technology Director or designee to confirm that the device is equipped with up-to-date virus software, and is configured properly. Connection of any personal electronic device is subject to all procedures in this document.

UNACCEPTABLE NETWORK USE BY STAFF AND STUDENTS

- Personal gain, commercial solicitation, and compensation of any kind;
- Actions that result in liability or cost incurred by the district;
- Downloading, installation and use of games, audio files, video files, or other applications (including unauthorized applications, freemium software or browser extensions) without permission or approval from the Superintendent or designee;
- Support or opposition for ballot measures, candidates, and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;
- Unauthorized access to other district computers, networks, and information systems;
- Cyber-bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- Information posted, sent, or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- Accessing, uploading, downloading, storage and distribution of obscene, pornographic, or sexually explicit material;
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and additional disciplinary action may be taken;
- Intentionally wasting limited resources. The District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence or any other errors or omissions.

The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the District's computer network or the Internet.

INTERNET SAFETY

Personal Information and Inappropriate Content

- Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail, or as content on any other electronic medium;
- Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
- No student pictures or names can be published on any public class, school, or district web site unless the appropriate permission has been obtained according to district policy; and
- If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

FILTERING AND MONITORING

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). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;

- Any attempts to defeat or bypass the District's Internet filter or conceal Internet activity are prohibited: (e.g., proxies, https, special ports, modifications to district browser settings, and any other techniques designed to evade filtering or enable the publication of inappropriate content);
- E-mail inconsistent with the educational and research mission of the District will be considered SPAM and blocked from entering district e-mail boxes;
- The District will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district devices;
- Staff members who supervise students, control electronic equipment, or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively.

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.

- Age appropriate materials will be made available for use across grade levels.
- Training on online safety issues and materials implementation will be made available for administration, staff, and families.

COPYRIGHT

Downloading, copying, duplicating and distributing software, music, sound files, movies, images, or other 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.

OWNERSHIP OF WORK

All work completed by employees as part of their employment will be considered property of the District. The District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the District, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

NETWORK SECURITY AND PRIVACY
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 for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

- Enroll in Multi-Factor Authentication for device and account access
- 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 user account password, keep it in a secure location;
- 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.

Student Data is Confidential

District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

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.

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 record 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, field trips, lunch supervision, etc. Furthermore, to respect workplace civility and privacy, these devices may not be used to record 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 building administration.

- Future-Proofing: This policy applies to all current and future wearable technologies with similar capabilities, regardless of brand or form.

No Expectation of Privacy

The District provides the network system, e-mail, and Internet access as a tool for education and research in support of the District's mission. 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.

No student or staff user should have any expectation of privacy when using the District's network. Communications may not be encrypted so as to avoid a security review. The District reserves the right to disclose any electronic messages to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the state of Washington.

Archive and Backup

Backup is made of all district e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on district servers regularly. Refer to the District's retention policy for specific records retention requirements.

Disciplinary Action

All users of the District's electronic resources are required to comply with the District's policy and procedures (and agree to abide by the provisions set forth in the District's user agreement). Violation of any of the conditions of use explained in the District's user agreement, Electronic Resources Policy, or in these procedures could be cause for disciplinary action, including suspension or expulsion from school, and suspension or revocation of network and computer access privileges.